



King's Research Portal

DOI:

[10.1017/S0305004118000075](https://doi.org/10.1017/S0305004118000075)

Document Version

Peer reviewed version

[Link to publication record in King's Research Portal](#)

Citation for published version (APA):

Betts, L. A., Dokshitser, V., & Morgan, A. (2018). Variation of Tamagawa numbers of semistable abelian varieties in field extensions. *MATHEMATICAL PROCEEDINGS- CAMBRIDGE PHILOSOPHICAL SOCIETY*. <https://doi.org/10.1017/S0305004118000075>

Citing this paper

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

Take down policy

If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

VARIATION OF TAMAGAWA NUMBERS OF SEMISTABLE ABELIAN VARIETIES IN FIELD EXTENSIONS

L. ALEXANDER BETTS, VLADIMIR DOKCHITSER

(with an appendix by V. Dokchitser and A. Morgan)

ABSTRACT. We investigate the behaviour of Tamagawa numbers of semistable principally polarised abelian varieties in extensions of local fields. In particular, we give a simple formula for the change of Tamagawa numbers in totally ramified extensions and one that computes Tamagawa numbers up to rational squares in general extensions. As an application, we extend some of the existing results on the p -parity conjecture for Selmer groups of abelian varieties by allowing more general local behaviour. We also give a complete classification of the behaviour of Tamagawa numbers for semistable 2-dimensional principally polarised abelian varieties that is similar to the well-known one for elliptic curves. The appendix explains how to use this classification for Jacobians of genus 2 hyperelliptic curves given by equations of the form $y^2 = f(x)$, under some simplifying hypotheses.

CONTENTS

1. Introduction	2
1.1. Tamagawa numbers	2
1.2. Semistable reduction types in toric dimension ≤ 2	3
1.3. The p -parity conjecture	4
1.4. Method of proof	6
1.5. Notation	9
2. C_k -lattices and the group $(\Lambda^\vee/\Lambda)^{C_k}$	9
2.1. The main formula	10
2.2. Properties of \mathfrak{B}_Λ and $H^1(C_k, \Lambda)$	11
2.3. Explicit descriptions of \mathfrak{B}_Λ and $H^1(C_k, \Lambda)$	13
2.4. Growth in towers (up to squares)	15
2.5. Examples	18
2.6. Classification of rank 1 and 2 lattices	19
3. Tamagawa numbers of semistable abelian varieties	22
3.1. Character group $\Lambda_{A/K}$	22
3.2. Behaviour of Tamagawa numbers in field extensions	23
3.3. Classification for dimension 2	26
3.4. Applications to the p -parity conjecture	28
4. Appendix: Integral module structure of $\Lambda_{A/K}$ for Jacobians of semistable hyperelliptic curves of genus 2	33
References	35

2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 11G25, 11G40, 14K15, 20C10.

1. INTRODUCTION

This article studies local Tamagawa numbers of abelian varieties over p -adic fields, and how these change as one makes the field larger. We focus on the relatively simple case of semistable abelian varieties. However, it is crucial to us that the residue field of the base field is not algebraically closed, in which respect our focus differs from many works, such as [9, 11] or more recently [8]. Indeed, the origin of our investigation comes from the study of Selmer groups and questions related to the Birch–Swinnerton-Dyer conjecture, the parity conjecture and Iwasawa theory, where the abelian varieties live over number fields and the local terms, such as Tamagawa numbers, are computed over their completions. One of our main applications is an extension of the results of [3] on the p -parity conjecture.

1.1. Tamagawa numbers. The theorem below illustrates the type of results on Tamagawa numbers that we obtain; the full list is given in §3.2. Let A be a semistable abelian variety over a p -adic field, that is, a finite extension K of \mathbb{Q}_p . We write $c_{A/K}$ for its Tamagawa number. Recall that the *toric dimension* d of A/K is the dimension of the torus in its Raynaud parametrisation (see §1.4), and its *split toric dimension* r is the dimension of the “split part of the torus”, more precisely the rank of the $\text{Gal}(K^{nr}/K)$ -fixed sublattice of the character group of the torus. Equivalently, r is the multiplicity of 1 as an eigenvalue of the Frobenius element in its action on the Tate module $T_\ell(A/K)$ or on $H_{\text{ét}}^1(A_{\overline{K}}, \mathbb{Q}_\ell)$ for any $\ell \neq p$, and d is the total number, counting multiplicities, of Frobenius eigenvalues of absolute value 1. To describe the behaviour of Tamagawa numbers we also introduce a finite abelian group $\mathfrak{B}_{A/K}$, whose definition will be given in §1.4.

Theorem 1.1.1 (Variation of Tamagawa numbers in field extensions). *Let K be a finite extension of \mathbb{Q}_p , and A/K a semistable principally polarised abelian variety of toric dimension d and split toric dimension r .*

(i) *If L/K is a totally ramified extension of degree e , then*

$$c_{A/L} = |\mathfrak{B}_{A/K}[e]| \cdot c_{A/K} \cdot e^r.$$

(ii) *If $K \subset L_1 \subset L_2 \subset \dots$ is a tower of finite extensions with L_t/K of ramification degree e_t , then for all sufficiently large t*

$$c_{A/L_t} = C \cdot e_t^{r_\infty},$$

for some suitable constant $C \in \mathbb{Q}$, and where r_∞ is the split toric dimension of A/L_t for all sufficiently large t .

(iii) *If L/K is a finite extension of residue degree f and ramification degree e , then*

$$c_{A/L} \sim \begin{cases} c_{A/K} \cdot e^r & \text{if } 2 \nmid e, 2 \nmid f, \\ c_{A/K} \cdot |\mathfrak{B}_{A/K}| \cdot e^r & \text{if } 2 \mid e, 2 \nmid f, \\ c_{A/K^{nr}} \cdot e^d & \text{if } 2 \mid f, \end{cases}$$

where \sim denotes equality up to rational squares.

Note that point (i) interprets $\mathfrak{B}_{A/K}$ number-theoretically, as the group that controls the Tamagawa number $c_{A/L}$ in totally ramified extensions L/K . Points (ii) and (iii) were motivated by, respectively, Iwasawa theoretic considerations (see [5] Thm. 5.5) and applications to the p -parity conjecture that require knowing the behaviour of Birch–Swinnerton-Dyer quotients up to rational squares in field extensions (see §1.3 below, and §3.4).

It is worth remarking that for the purposes of point (ii) the assumption that A/K admits a principal polarisation may be removed (see Corollary 3.2.8). However, the semistability assumption is necessary to obtain such a stable growth: for example, the Tamagawa number of the elliptic curve 243a1 fluctuates between 1 and 3 in the layers of the cyclotomic \mathbb{Z}_3 -tower of \mathbb{Q}_3 , see [5] Remark 5.4.

1.2. Semistable reduction types in toric dimension ≤ 2 . We also apply our techniques to study in detail semistable abelian varieties that have toric dimension ≤ 2 (see §3.3), giving a complete classification of possible reduction types and their behaviour in field extensions. This is summarised in the theorem below, which is a direct consequence of Theorems 2.6.2 and 3.3.2. It is worth pointing out that this is an altogether different kind of classification from that of Namikawa–Ueno [11] for curves of genus 2, since we treat only the semistable case, but, on the other hand, are very much interested in the action of the Frobenius element.

We will classify reduction types of principally polarised semistable abelian varieties in terms of the character lattice $\Lambda_{A/K}$ of the torus in the Raynaud parametrisation of A/K (see §1.4 for details). It comes with a natural embedding into its dual lattice $\Lambda_{A/K} \hookrightarrow \Lambda_{A/K}^\vee$ and with an action of the Frobenius element $\text{Fr} \in \text{Gal}(K^{nr}/K)$ as an automorphism of finite order. This data is, in particular, sufficient to recover the Tamagawa number.

To motivate our classification result, let us first recall the corresponding classification for elliptic curves:

Example 1.2.1. Let K/\mathbb{Q}_p be a finite extension and E/K an elliptic curve with multiplicative reduction. The elliptic curve has Kodaira type I_n for some $n \geq 1$, and either split or non-split multiplicative reduction. If L/K is a finite extension of residue degree f and ramification degree e , then E/L has Kodaira type I_{en} and the split/non-split characteristic is the same as for E/K unless f is even, in which case the reduction is always split over L . The reduction type is related to the Frobenius action (denoted Fr) on $\Lambda_{E/K}$ and $\Lambda_{E/K}^\vee$ as follows:

Type	$\Lambda_{E/K}$	$\Lambda_{E/K}^\vee$	Fr	$c_{E/K}$	$f = 2$	condition
I_n split	\mathbb{Z}	$\frac{1}{n}\mathbb{Z}$	1	n	unchanged	
I_n non-split	\mathbb{Z}	$\frac{1}{n}\mathbb{Z}$	-1	$\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}$	I_n split	$\begin{smallmatrix} n \text{ odd} \\ n \text{ even} \end{smallmatrix}$

The table also lists the corresponding Tamagawa number and the effect of a quadratic unramified extension (under “ $f = 2$ ”). Note that together with the fact that an unramified extension of odd degree does not change the reduction type and the knowledge of the effect of a totally ramified extension, the table is sufficient to determine the reduction type of E/L and its Tamagawa number for every finite extension L/K .

Note also that the above classification applies more generally to semistable abelian varieties of toric dimension 1: $\Lambda_{A/K}$ is then isomorphic to \mathbb{Z} , $\Lambda_{A/K}^\vee$ is some lattice containing Λ with finite index (hence $= \frac{1}{n}\mathbb{Z}$) and Fr is an automorphism of $\Lambda_{A/K}$ (hence multiplication by ± 1). As explained in §1.4, the Tamagawa number is given by $|(\frac{1}{n}\mathbb{Z}/\mathbb{Z})^{\text{Fr}}|$, and the behaviour in ramified and unramified extensions is obtained by scaling by e or replacing Fr by Fr^f . Thus the overall result is exactly as for elliptic curves with multiplicative reduction.

The theorem below gives an analogous table for toric dimension ≤ 2 ; in particular, it covers Jacobians of all semistable curves of genus 2. The appendix (§4) explains how to explicitly determine the type of the Jacobian of a genus 2 hyperelliptic curve given by an equation of the form $y^2 = f(x)$ over a finite extension of \mathbb{Q}_p , assuming that p is odd and that $f(x)$ is integral with a unit leading coefficient and no triple roots over the residue field.

Theorem 1.2.2. *Let K/\mathbb{Q}_p be a finite extension and let A/K be a semistable principally polarised abelian variety of toric dimension ≤ 2 .*

Then, up to Fr-equivariant isomorphism, $\Lambda_{A/K}, \Lambda_{A/K}^\vee$ are given by one of the cases in the following table. The parameters n and m are strictly positive integers. All the types are distinct, except for $[1.1 : n, m]$ and $[1.1 : n', m']$ which are isomorphic if and only if $C_n \times C_m \simeq C_{n'} \times C_{m'}$, and similarly for $[2.2 : n, m]$ and $[2.2 : n', m']$. The Tamagawa number $c_{A/K}$ is determined by the type as shown in the table.

Type	$\Lambda_{A/K}$	$\Lambda_{A/K}^\vee$	Fr	$f = 3$	$f = 2$	$c_{A/K}$
good	0	0	1	unchanged	unchanged	1
$[1 : n]$	\mathbb{Z}	$\frac{1}{n}\mathbb{Z}$	1	unchanged	unchanged	n
$[2 : n]$	\mathbb{Z}	$\frac{1}{n}\mathbb{Z}$	-1	unchanged	$[1 : n]$	1 (n odd) 2 (n even)
$[1.1 : n, m]$	\mathbb{Z}^2	$\frac{1}{n}\mathbb{Z} \oplus \frac{1}{m}\mathbb{Z}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	unchanged	unchanged	nm
$[1.2_A : n, m]$	\mathbb{Z}^2	$\frac{1}{n}\mathbb{Z} \oplus \frac{1}{m}\mathbb{Z}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	unchanged	$[1.1 : n, m]$	n (m odd) $2n$ (m even)
$[1.2_B : n, m]$ $n \equiv m \pmod{2}$	$\mathbb{Z}^2 + \langle \frac{1}{2}, \frac{1}{2} \rangle$	$\frac{1}{n}\mathbb{Z} \oplus \frac{1}{m}\mathbb{Z} + \langle \frac{1}{2n}, \frac{1}{2m} \rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	unchanged	$[1.1 : 2n, \frac{m}{2}]$ $[1.1 : n, m]$ $[1.1 : \frac{n}{2}, 2m]$	n ($\text{ord}_2 \frac{n}{m} > 0$) n ($\text{ord}_2 \frac{n}{m} = 0$) n ($\text{ord}_2 \frac{n}{m} < 0$)
$[2.2 : n, m]$	\mathbb{Z}^2	$\frac{1}{n}\mathbb{Z} \oplus \frac{1}{m}\mathbb{Z}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	unchanged	$[1.1 : n, m]$	1 (n, m odd) 2 (n, m odd/even) 4 (n, m even)
$[3 : n]$	$\mathbb{Z}[\zeta_3]$	$\frac{\zeta_3 - 1}{3n}\mathbb{Z}[\zeta_3]$	$\cdot \zeta_3$	$[1.1 : n, 3n]$	unchanged	3
$[4 : n]$	$\mathbb{Z}[i]$	$\frac{1}{n}\mathbb{Z}[i]$	$\cdot i$	unchanged	$[2.2 : n, n]$	1 (n odd) 2 (n even)
$[6 : n]$	$\mathbb{Z}[\zeta_3]$	$\frac{\zeta_3 - 1}{3n}\mathbb{Z}[\zeta_3]$	$\cdot \zeta_6$	$[2.2 : n, 3n]$	$[3 : n]$	1

If L/K is an unramified extension of degree coprime to 2 and 3 then A/L has the same type with the same parameters n, m as A/K . If L/K is an unramified extension of degree 2 or 3 then the type of A/L changes as shown in the table under the headings “ $f = 2$ ” and “ $f = 3$ ”, respectively. Finally, if L/K is a totally ramified extension of degree e , then A/L has the same type as A/K with parameters n and m replaced by en and em .

1.3. The p -parity conjecture. Finally, we turn to an application to the p -parity conjecture for abelian varieties, which is a parity version of the Birch–Swinnerton-Dyer conjecture.

Let A/K be an abelian variety over a number field. Its main arithmetic invariant is its Mordell–Weil rank, that is, the rank of its group of K -rational points $A(K)$.

The Birch–Swinnerton-Dyer conjecture predicts that this coincides with the analytic rank of A/K — the order of vanishing at $s = 1$ of the L -function $L(A/K, s)$. Since the L -function is conjectured to satisfy a functional equation of the type $s \leftrightarrow 2 - s$, the parity of the analytic rank can be read off from the sign in the functional equation: it is even if the sign is $+$ and odd if the sign is $-$. This sign is (conjecturally) explicitly given as the root number $w(A/K)$, which is constructed via the theory of local root numbers or local ϵ -factors, and hence one can talk about the “parity of the analytic rank” without knowing that the L -function has an analytic continuation to $s = 1$. The Parity Conjecture is precisely this parity version of the Birch–Swinnerton-Dyer Conjecture, i.e. that the parity of the rank of A/K can be read off from the root number as $(-1)^{\text{rk } A/K} = w(A/K)$.

Moreover, if F/K is a Galois extension, then one can try to determine the multiplicities of the irreducible constituents in the representation $A(F) \otimes_{\mathbb{Z}} \mathbb{C}$ of $\text{Gal}(F/K)$. A generalisation of the Birch–Swinnerton-Dyer conjecture predicts that the multiplicity of a (complex) irreducible representation τ is given by the order of vanishing of the twisted L -function $L(A/K, \tau, s)$ at $s = 1$, see e.g. [14] §2. Once again, there is a parity conjecture to the effect that, for self-dual τ , the parity of this multiplicity can be recovered from the associated root number as $(-1)^{\langle \tau, A(K) \otimes \mathbb{C} \rangle} = w(A/K, \tau)$, where $\langle \cdot, \cdot \rangle$ is the usual inner product of characters.

In view of the conjectured finiteness of the Tate-Shafarevich group $\text{III}(A/K)$, there is also the following p -parity conjecture, that morally ought to be more accessible, although still remains unresolved. For a prime number p let

$$\mathcal{X}_p(A/K) = (\text{Pontryagin dual of the } p^\infty\text{-Selmer group of } A/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

This is a \mathbb{Q}_p -vector space whose dimension is the rank of A/K , provided $\text{III}(A/K)$ is finite; in general $\dim_{\mathbb{Q}_p} \mathcal{X}_p(A/K) = \text{rk } A/K + t$, where t measures the p -divisible part of III as $\text{III}(A/K)[p^\infty] = (\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus t} \oplus (\text{finite group})$. Then we expect:

Conjecture 1.3.1 (p -Parity Conjecture). *For an abelian variety over a number field A/K ,*

$$(-1)^{\dim \mathcal{X}_p(A/K)} = w(A/K).$$

If F/K is a Galois extension and τ a self-dual representation of $\text{Gal}(F/K)$, then

$$(-1)^{\langle \tau, \mathcal{X}_p(A/F) \rangle} = w(A/K, \tau).$$

The second formula is a strictly stronger statement, as taking $\tau = \mathbf{1}$ recovers the first one. We will refer to it as the p -parity conjecture for the twist of A/K by τ .

Most results on the p -parity conjecture concern elliptic curves; in particular the first formula is now known to hold for all elliptic curves over \mathbb{Q} and in many cases for elliptic curves over totally real fields [4, 12]. The situation with general abelian varieties is more difficult, and the main results are those of [2] that establish the first formula assuming that the abelian variety admits a suitable isogeny, and of [3] that proves the second formula for a class of representations τ . Our results on the behaviour of Tamagawa numbers let us strengthen the results of the latter paper as follows.

For a Galois extension of number fields F/K and a prime number p , the “regulator constant” machinery of [3] and its preceding papers constructs a special set $\mathbf{T}_p^{F/K}$ of self-dual representations of $\text{Gal}(F/K)$. Unfortunately there is still no simple description of the set $\mathbf{T}_p^{F/K}$; we refer the reader to §3.4 for its definition. We will prove the following result on the p -parity conjecture for twists by $\tau \in \mathbf{T}_p^{F/K}$.

It effectively removes the ugly assumption “4ex” and the extra hypothesis on the polarisation from [3] Thm. 3.2 and its applications. Strictly speaking this is only a strengthening of existing results for the one prime $p=2$. However, 2-Selmer groups have been particularly important for the parity conjectures, explicit descent, quadratic twists, as well as recent results on hyperelliptic curves [1].

Theorem 1.3.2. *Let F/K be a Galois extension of number fields and let p be a prime number. Let A/K be a principally polarised abelian variety all of whose primes of non-semistable reduction have cyclic decomposition groups¹ in F/K . Then*

- (1) *The p -parity conjecture holds for all twists of A/K by $\tau \in \mathbf{T}_p^{F/K}$.*
- (2) *If $\mathrm{Gal}(F/K) \simeq D_{2p^n}$, then the p -parity conjecture holds for A/K twisted by τ of the form $\tau = \sigma \oplus \mathbf{1} \oplus \det \sigma$ for every 2-dimensional representation σ of $\mathrm{Gal}(F/K)$. (Here D_{2k} denotes the dihedral group of order $2k$.)*
- (3) *Suppose $p = 2$ and that the 2-Sylow subgroup of $\mathrm{Gal}(F/K)$ is normal. If the 2-parity conjecture holds for A/K and over all quadratic extensions of K in F , then it holds for A over all subfields of F and for all twists of A by orthogonal representations of $\mathrm{Gal}(F/K)$.*

Let us stress that the theorem provides a large number of twists of A/K for which the p -parity conjecture holds: for example we could prove the p -parity conjecture for all principally polarised abelian varieties A over \mathbb{Q} using (2) if we knew how to find a D_{2p} -extension of \mathbb{Q} in which (i) the p^∞ -Selmer rank of A does not grow, (ii) the analytic rank of A does not grow, or at least $w(A, \sigma) = w(A, \det \sigma) = 1$ for a faithful 2-dimensional representation σ , and (iii) the primes of non-semistable reduction of A are unramified. (Here D_4 should be interpreted as $C_2 \times C_2$ for $p = 2$.)

Part (1) will be proved in Theorem 3.4.10. Part (2) then follows from [3] Ex. 2.21, 2.22 that compute regulator constants for dihedral groups (same as in [3] Thm. 4.2). Similarly (3) follows from [3] Thm. 4.4, Thm. 4.5., where “Hypothesis 4.1” holds by (2).

Remark 1.3.3. Adam Morgan has recently proved that the 2-parity conjecture holds after a proper quadratic extension of the base field for Jacobians of hyperelliptic curves, under some local conditions on the reduction types [10]. Thus in Theorem 1.3.2 (3) for this class of abelian varieties one only needs to assume the 2-parity conjecture for A/K itself.

1.4. Method of proof. In order to perform the Tamagawa number computations for the proof of Theorem 1.1.1, we will use the theory of the Raynaud parametrisation, thereby reducing the problem to one of pure algebra. Specifically (see §3 or [3] §3.5.1 for further details), if A/K is an abelian variety over a p -adic field with split semistable reduction, then the character lattice $\Lambda_{A/K}$ of the toric part of the Raynaud parametrisation of A is a finite rank free \mathbb{Z} -module endowed with a non-degenerate symmetric pairing $\Lambda_{A/K} \otimes \Lambda_{A/K} \rightarrow \mathbb{Z}$ induced from the monodromy pairing and the principal polarisation. This pairing on $\Lambda_{A/K}$ induces an embedding $\Lambda_{A/K} \hookrightarrow \Lambda_{A/K}^\vee$ into the dual lattice, and the Tamagawa number of A/K is given by the order of the quotient $\Lambda_{A/K}^\vee / \Lambda_{A/K}$.

¹e.g. if they are unramified

More generally, if the reduction of A is semistable but not necessarily split, then it becomes split after some finite unramified extension K'/K and hence the lattice $\Lambda_{A/K} := \Lambda_{A/K'}$ (which is independent of K') carries an action of $\text{Gal}(K'/K)$ (generated by Frobenius Fr), making the pairing on $\Lambda_{A/K}$ Galois-invariant. Hence the embedding $\Lambda_{A/K} \hookrightarrow \Lambda_{A/K}^\vee$ is $\text{Gal}(K'/K)$ -equivariant, and the Tamagawa number is given by

$$c_{A/K} = \left| \left(\frac{\Lambda_{A/K}^\vee}{\Lambda_{A/K}} \right)^{\text{Fr}} \right|.$$

If one replaces K by a finite extension L/K of ramification degree e and residue class degree f , then one can identify $\Lambda_{A/L}$ with $\Lambda_{A/K}$ in such a way that the pairing on $\Lambda_{A/L}$ is the pairing on $\Lambda_{A/K}$ scaled by a factor of e , and the action of Frobenius on $\Lambda_{A/L}$ agrees with the action of Fr^f on $\Lambda_{A/K}$. Hence, the numbers

$$\left| \left(\frac{\Lambda_{A/K}^\vee}{e\Lambda_{A/K}} \right)^{\text{Fr}^f} \right|$$

compute the Tamagawa numbers of A over all finite extensions L/K .

Thus the problem of understanding the growth of Tamagawa numbers in finite extensions reduces to a purely algebraic one, at least in the semistable case. We have a lattice Λ carrying a finite order automorphism Fr and a non-degenerate Fr -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$, and we are interested in the numbers $|(\Lambda^\vee/e\Lambda)^{\text{Fr}^f}|$ as e and f vary. The study of such lattices will be the focus of §2.

Initially, we will focus our attention on understanding the dependence on e , i.e. examining the case $f = 1$. To see the kinds of behaviour that can occur consider the following examples for $\Lambda = \mathbb{Z}^{\oplus 2}$ — rather than specifying the pairing on Λ we will for simplicity just specify the overlattice $\Lambda^\vee \geq \Lambda$, though all the examples given can be induced by at least one pairing.

(i) First take $\Lambda^\vee = \Lambda$ and Fr the identity map. Then $\Lambda^\vee/e\Lambda$ is, of course, all Fr -invariant and its order grows as $e^2 = e^{\text{rk}(\Lambda^{\text{Fr}})}$; in general the sublattice of Fr -invariants Λ^{Fr} will always contribute to $(\Lambda^\vee/e\Lambda)^{\text{Fr}}$ with precisely this kind of growth as e varies. (ii) Next suppose that Λ^\vee is the “diagonal” index 2 overlattice of Λ , that is, the span of the vectors $(1/2, 1/2)$ and $(1/2, -1/2)$. In this case both points of Λ^\vee/Λ must be Fr -invariant, even if Fr has no invariants on Λ itself. Note that these survive as Fr -invariants in $\Lambda^\vee/e\Lambda \cong \frac{1}{e}\Lambda^\vee/\Lambda$, and hence give a constant contribution as e varies. (iii) Finally, consider $\Lambda^\vee = \Lambda$ and Fr the multiplication by -1 map. When e is odd, $(\Lambda^\vee/e\Lambda)^{\text{Fr}} = (\Lambda^\vee/e\Lambda)[2]$ is trivial, but when e is even $(0, 0), (\frac{e}{2}, 0), (0, \frac{e}{2})$ and $(\frac{e}{2}, \frac{e}{2})$ are elements of order 2 in $\Lambda^\vee/e\Lambda$ and are, perforce, Fr -invariant. In other words, $\Lambda^\vee/e\Lambda$ can pick up a few sporadic Fr -invariants when e becomes divisible by a certain integer.

It turns out that these are the only types of contributions to $|(\Lambda^\vee/e\Lambda)^{\text{Fr}}|$. The third type of behaviour above will prove the most subtle to deal with, and to this end we introduce a finite group \mathfrak{B}_Λ which will control such contributions (for example, in the particular case that $\Lambda^\vee = \Lambda$, we will have $\mathfrak{B}_\Lambda = H^1(C_k, \Lambda)$; this precisely recovers the group $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ of 2-torsion points in example (iii).).

Definition 1.4.1. Let Λ be a lattice endowed with an action by a cyclic group $C_k = \langle \text{Fr} \rangle$ and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. This

induces a C_k -equivariant map $\Lambda \hookrightarrow \Lambda^\vee$, and we denote by

$$\mathfrak{B}_\Lambda := \text{im} \left(H^1(C_k, \Lambda) \rightarrow H^1(C_k, \Lambda^\vee) \right)$$

the image of the induced map on cohomology.

For a principally polarised semistable abelian variety A/K , we write

$$\mathfrak{B}_{A/K} = \mathfrak{B}_{\Lambda_{A/K}},$$

the group appearing in Theorem 1.1.1.

The general result that we will prove is the following:

Theorem 1.4.2. *Suppose that Λ is a lattice endowed with an action of a finite cyclic group $C_k = \langle \text{Fr} \rangle$, and with a non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Then*

$$\left| \left(\frac{\Lambda^\vee}{\Lambda} \right)^{\text{Fr}} \right| = \left| \frac{(\Lambda^\vee)^{\text{Fr}}}{\Lambda^{\text{Fr}}} \right| \cdot \frac{|H^1(C_k, \Lambda)|}{|\mathfrak{B}_\Lambda|},$$

and for all $e \geq 1$,

$$\left| \left(\frac{\Lambda^\vee}{e\Lambda} \right)^{\text{Fr}} \right| = \left| \left(\frac{\Lambda^\vee}{\Lambda} \right)^{\text{Fr}} \right| \cdot |\mathfrak{B}_\Lambda[e]| \cdot e^{\text{rk}(\Lambda^{\text{Fr}})}.$$

Remark 1.4.3. In sections 2.2 and 2.3, we will prove various properties of the groups $H^1(C_k, \Lambda)$ and \mathfrak{B}_Λ which often allow one to determine them in practice. Most notably, the group \mathfrak{B}_Λ admits a perfect antisymmetric pairing, and the order (respectively exponent) of both \mathfrak{B}_Λ and $H^1(C_k, \Lambda)$ is bounded in terms of the characteristic (respectively minimal) polynomial of Fr . Additionally, the order of $H^1(C_k, \Lambda)$ can be straightforwardly calculated in terms of this characteristic polynomial and a certain finite group \mathcal{T}_Λ , measuring the failure of Λ to decompose as the direct sum of the invariants Λ^{Fr} and their orthogonal complement.

When it comes to understanding the dependence on f of the quantity $|(\Lambda^\vee/e\Lambda)^{\text{Fr}^f}|$, we will not be quite so explicit, and will instead focus on describing $|(\Lambda^\vee/e\Lambda)^{\text{Fr}^f}|$ up to squares, as this will suffice for our application to the p -parity conjecture. It is here that the antisymmetric perfect pairing on \mathfrak{B}_Λ will play a vital role, since this forces $|\mathfrak{B}_\Lambda|$ to be either square or twice a square. Using variations on this idea, we will prove the following result, completely characterising $|(\Lambda^\vee/e\Lambda)^{\text{Fr}^f}|$ up to squares:

Theorem 1.4.4 (=Theorem 2.4.2). *Let Λ be a lattice endowed with an action by a cyclic group $C_k = \langle \text{Fr} \rangle$ and non-degenerate Fr -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Then for all $e, f \in \mathbb{N}$*

$$\left| (\Lambda^\vee/e\Lambda)^{\text{Fr}^f} \right| \sim \begin{cases} |(\Lambda^\vee/\Lambda)^{\text{Fr}}| \cdot e^{\text{rk}(\Lambda^{\text{Fr}})} & \text{if } 2 \nmid e, 2 \nmid f, \\ |(\Lambda^\vee/\Lambda)^{\text{Fr}}| \cdot |\mathfrak{B}_\Lambda| \cdot e^{\text{rk}(\Lambda^{\text{Fr}})} & \text{if } 2 \mid e, 2 \nmid f, \\ |\Lambda^\vee/\Lambda| \cdot e^{\text{rk}(\Lambda)} & \text{if } 2 \mid f. \end{cases}$$

The reader will note that this already implies point (iii) of Theorem 1.1.1.

1.5. Notation. In this paper, a *lattice* Λ will simply mean a finitely generated free abelian group, $\Lambda \simeq \mathbb{Z}^n$. It will often come with a non-degenerate symmetric pairing $(\cdot, \cdot) : \Lambda \otimes \Lambda \rightarrow \mathbb{Z}$, but in such cases we will always explicitly state it.

Throughout the paper, we use the notation:

M^F	F -invariants of M , i.e. $\{m \in M \mid Fm = m\}$ for an automorphism F
M^G	G -invariants of M , i.e. $\{m \in M \mid gm = m \forall g \in G\}$ for a group G
$M[e]$	e -torsion of M , i.e. $\{m \in M \mid em = 0\}$ for $e \in \mathbb{Z}$
Λ^\vee	dual lattice to Λ , i.e. $\text{Hom}(\Lambda, \mathbb{Z})$
Λ^\vee / Λ	cokernel of the map $\Lambda \rightarrow \Lambda^\vee$ induced by a symmetric pairing on Λ
ζ_k	primitive k -th root of unity
\mathcal{T}_Λ	see Definition 2.3.1
\mathfrak{B}_Λ	see Definition 1.4.1

For a finite extension K/\mathbb{Q}_p and an abelian variety A/K we use the notation:

K^{nr}	maximal unramified extension of K
Fr	Frobenius element (in §3)
$c_{A/K}$	local Tamagawa number of A/K
$w(A/K)$	local root number of A/K
$w(A/K, \tau)$	local root number of the twist of A by τ , see [15]
$\Lambda_{A/K}$	see Notation 3.1.1
$\mathfrak{B}_{A/K}, \mathcal{T}_{A/K}, P_{A/K}$	see Notation 3.2.1

Note that we use the same notation for global root numbers when K is a number field. In this setting we also write $\mathcal{X}_p(A/K)$ for the dual p^∞ -Selmer group of A/K (see §1.3), that is,

$$\mathcal{X}_p(A/K) = \text{Hom}_{\mathbb{Z}_p}(\varinjlim \text{Sel}_{p^n}(A/K), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p.$$

Remark 1.5.1. One can carry out the algebraic analysis in the greater generality when the action of the finite group C_k is replaced by the action of an endomorphism whose minimal polynomial has no repeated root at 1, for instance generalising the definition of \mathfrak{B}_Λ and proving an analogue of Theorem 1.4.2. The details can be found in version 3 of the arXiv preprint of this paper.

Acknowledgements. We would like to thank the referee for their very careful reading of this manuscript, and for describing how to use cohomological arguments to significantly simplify the proofs in section 2.2. We are also grateful to Tim Dokchitser and Adam Morgan for their useful comments. We would also like to thank Emmanuel College and Trinity College, Cambridge, where most of this research was carried out. The second author is supported by a Royal Society University Research Fellowship.

2. C_k -LATTICES AND THE GROUP $(\Lambda^\vee / \Lambda)^{C_k}$

In this section we examine on an abstract level the lattices Λ (with unramified Galois action and pairing) of the type that arise as character lattices of the toric part of the Raynaud parametrisation of semistable principally polarised abelian varieties. Specifically, we will be considering finitely-generated free \mathbb{Z} -modules Λ endowed with a action by a finite cyclic group C_k and with a non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$.

We will be particularly interested in the quantity

$$|(\Lambda^\vee / \Lambda)^{C_k}|,$$

which, when Λ arises from an abelian variety as above, computes its Tamagawa number. Our methods for accessing this quantity are mainly cohomological, and focus on the finite group \mathfrak{B}_Λ defined in Definition 1.4.1. Besides being closely related to the quantity $|(\Lambda^\vee/\Lambda)^{C_k}|$ of interest, the key property of this group is that it admits an antisymmetric perfect pairing (valued in the Pontryagin dual C_k^* , non-canonically isomorphic to $\mathbb{Z}/k\mathbb{Z}$), and it is this which allows us to get fine control on Tamagawa numbers up to squares.

The main formula we will be using is the following, describing the quantity $|(\Lambda^\vee/\Lambda)^{C_k}|$ of interest as a product of natural quantities, and it is this formula which allows us to understand the growth of $|(\Lambda^\vee/e\Lambda)^{C_k}|$ as e varies.

2.1. The main formula.

Theorem 2.1.1. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Then*

$$\left| \left(\frac{\Lambda^\vee}{\Lambda} \right)^{C_k} \right| = \frac{|(\Lambda^\vee)^{C_k}/\Lambda^{C_k}| \cdot |H^1(C_k, \Lambda)|}{|\mathfrak{B}_\Lambda|}.$$

Proof. The short exact sequence

$$0 \rightarrow \Lambda \rightarrow \Lambda^\vee \rightarrow \Lambda^\vee/\Lambda \rightarrow 0$$

yields a cohomology exact sequence

$$0 \rightarrow (\Lambda^\vee)^{C_k}/\Lambda^{C_k} \rightarrow (\Lambda^\vee/\Lambda)^{C_k} \rightarrow H^1(C_k, \Lambda) \rightarrow \mathfrak{B}_\Lambda \rightarrow 0.$$

Since all the groups involved are finite (as $\Lambda^{C_k} \leq (\Lambda^\vee)^{C_k}$ full rank), we obtain the desired relation between sizes. \square

In order to control the quantity $|(\Lambda^\vee/e\Lambda)^{C_k}|$ as $e \in \mathbb{N}$ varies, we will use a variant of the formula in Theorem 2.1.1 which describes the dependence on e in terms of the group \mathfrak{B}_Λ . For this we require a preliminary proposition.

Proposition 2.1.2. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$, and let Λ_e be the lattice formed by scaling the pairing on Λ by a factor of $e \in \mathbb{N}$. Then*

$$\mathfrak{B}_{\Lambda_e} \cong \mathfrak{B}_\Lambda/\mathfrak{B}_\Lambda[e].$$

Proof. Scaling the pairing on Λ doesn't change either the underlying lattice Λ or Λ^\vee , but does scale the embedding $\Lambda \hookrightarrow \Lambda^\vee$, and hence the map $H^1(C_k, \Lambda) \rightarrow H^1(C_k, \Lambda^\vee)$, by a factor of e . Thus $\mathfrak{B}_{\Lambda_e} \cong e\mathfrak{B}_\Lambda \cong \mathfrak{B}_\Lambda/\mathfrak{B}_\Lambda[e]$, as desired. \square

Corollary 2.1.3. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Then for all $e \in \mathbb{N}$ we have*

$$|(\Lambda^\vee/e\Lambda)^{C_k}| = |(\Lambda^\vee/\Lambda)^{C_k}| \cdot e^{\text{rk}(\Lambda^{C_k})} \cdot |\mathfrak{B}_\Lambda[e]|.$$

Proof. Note that, in the notation of Proposition 2.1.2, $(\Lambda^\vee/e\Lambda)^{C_k} \cong (\Lambda^\vee/\Lambda_e)^{C_k}$. The result follows by applying Theorem 2.1.1 to Λ and to Λ_e . \square

Corollary 2.1.4. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Then $|(\Lambda^\vee/e\Lambda)^{C_k}|$, as a function of e , is of the form*

$$|(\Lambda^\vee/e\Lambda)^{C_k}| = a \cdot e^{r_1} \cdot \prod_q \prod_{s \geq 1} \text{hcf}(e, q^s)^{r_{q^s}}$$

for some $a \in \mathbb{N}$ and $r_{q^s} \in \mathbb{N}_0$ (indexed by prime powers). The indices r_{q^s} are almost all 0, and r_{q^s} is even for $q^s > 2$.

Proof. This is immediate from Corollary 2.1.3. The indices r_{q^s} for $q^s > 1$ are the structure constants from the decomposition $\mathfrak{B}_\Lambda \simeq \bigoplus_q \bigoplus_{s \geq 1} (\mathbb{Z}/q^s\mathbb{Z})^{\oplus r_{q^s}}$. We will see in Proposition 2.2.2 that \mathfrak{B}_Λ admits a perfect antisymmetric pairing, which gives the desired parity conditions on the r_{q^s} . \square

2.2. Properties of \mathfrak{B}_Λ and $H^1(C_k, \Lambda)$. In applying Theorem 2.1.1, it will be useful to understand the terms \mathfrak{B}_Λ and $H^1(C_k, \Lambda)$ and what sizes they can take. The key restriction comes from the antisymmetric perfect pairing on \mathfrak{B}_Λ , but we will also describe more general bounds on the order and exponent of \mathfrak{B}_Λ and $H^1(C_k, \Lambda)$.

We begin by examining the group $H^1(C_k, \Lambda)$. Throughout this section, we will repeatedly use the fact that cup-product pairings are graded-commutative: for any finite group G , G -modules A and B and elements $a \in H^j(G, A)$ and $b \in H^k(G, B)$ we have

$$b \cup a = (-1)^{jk} \tau_*(a \cup b),$$

where $\tau_*: H^{j+k}(G, A \otimes B) \xrightarrow{\sim} H^{j+k}(G, B \otimes A)$ is the canonical isomorphism induced by interchange of factors.

Proposition 2.2.1. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Write the characteristic (respectively minimal) polynomial of a generator σ as $\pm(t-1)^r P(t)$ with $P(1) > 0$ (respectively $\pm(t-1)^{r_0} P_0(t)$). Then:*

- $H^1(C_k, \Lambda)$ is a finite abelian group, with exponent dividing $P_0(1) \mid k$ and order dividing $P(1)$;
- the cup product pairing $H^1(C_k, \Lambda) \otimes H^1(C_k, \Lambda) \rightarrow H^2(C_k, \mathbb{Z})$ induced by the given pairing is antisymmetric (but not necessarily alternating);
- the cup product pairing $H^1(C_k, \Lambda^\vee) \otimes H^1(C_k, \Lambda) \rightarrow H^2(C_k, \mathbb{Z})$ induced by the evaluation pairing is perfect.

Proof. Let ${}_N\Lambda$ denote the kernel of the norm map $1 + \sigma + \cdots + \sigma^{k-1}$, which is a pure submodule of Λ . Then C_k acts without fixed points on ${}_N\Lambda$ and acts trivially on $\Lambda/{}_N\Lambda$, so that the characteristic (resp. minimal) polynomial of $\sigma|_{{}_N\Lambda}$ is $\pm P(t)$ (resp. $\pm P_0(t)$). In particular, $H^1(C_k, {}_N\Lambda)$ is isomorphic to the cokernel of $(\sigma - 1)$, so has order $P(1)$. Since it is annihilated by both $(\sigma - 1)$ and $P_0(\sigma)$, it has exponent dividing $P_0(1)$, and this divides k since $P_0(t)$ divides $\frac{t^k - 1}{t - 1}$.

Yet since $\Lambda/{}_N\Lambda$ is torsion-free with trivial C_k -action, the map on cohomology $H^1(C_k, {}_N\Lambda) \rightarrow H^1(C_k, \Lambda)$ is surjective, so $H^1(C_k, \Lambda)$ is also finite of order dividing $P(1)$ and exponent dividing $P_0(1)$, as desired.

The second point then follows from graded-commutativity of the cup product $H^1(C_k, \Lambda) \otimes H^1(C_k, \Lambda) \rightarrow H^2(C_k, \Lambda \otimes \Lambda)$ by postcomposing with the induced map $H^2(C_k, \Lambda \otimes \Lambda) \rightarrow H^2(C_k, \mathbb{Z})$ from the given pairing.

For the third point, we note that since $H^2(C_k, \mathbb{Z}) \cong H^1(C_k, \mathbb{Q}/\mathbb{Z}) \cong C_k^*$ embeds in \mathbb{Q}/\mathbb{Z} , it suffices to show that the pairing is left- and right-non-degenerate. Moreover, under the canonical isomorphism $(\Lambda^\vee)^\vee \cong \Lambda$, the evaluation pairing $\Lambda^\vee \otimes \Lambda \rightarrow \mathbb{Z}$ associated to Λ is identified with the evaluation pairing $\Lambda^\vee \otimes (\Lambda^\vee)^\vee \rightarrow \mathbb{Z}$ associated to Λ^\vee , with the factors interchanged, so that by graded-commutativity of the cup product it suffices to just prove non-degeneracy on the left.

To do this, suppose that $[\phi] \in H^1(C_k, \Lambda^\vee)$ is in the left-kernel of the cup product map. Since in the exact sequence of C_k -modules

$$0 \rightarrow \Lambda^\vee \rightarrow \text{Hom}(\Lambda, \mathbb{Q}) \rightarrow \text{Hom}(\Lambda, \mathbb{Q}/\mathbb{Z}) \rightarrow 0$$

the middle term has trivial H^1 , we can write $[\phi]$ as the image of $\psi \in \text{Hom}_{C_k}(\Lambda, \mathbb{Q}/\mathbb{Z})$ under the coboundary map $\delta: H^0(C_k, \text{Hom}(\Lambda, \mathbb{Q}/\mathbb{Z})) \rightarrow H^1(C_k, \Lambda^\vee)$.

Now by compatibility of cup products with coboundary maps, we have a commuting square

$$\begin{array}{ccc} H^0(C_k, \text{Hom}(\Lambda, \mathbb{Q}/\mathbb{Z})) \otimes H^1(C_k, \Lambda) & \longrightarrow & H^1(C_k, \mathbb{Q}/\mathbb{Z}) \\ \downarrow \delta \otimes 1 & & \downarrow \delta \\ H^1(C_k, \Lambda^\vee) \otimes H^1(C_k, \Lambda) & \longrightarrow & H^2(C_k, \mathbb{Z}) \end{array}$$

so that ψ is in the left-kernel of the top cup product map in the square. Concretely, this means that for any 1-cocycle $C_k \rightarrow \Lambda$, the composite $C_k \rightarrow \Lambda \xrightarrow{\psi} \mathbb{Q}/\mathbb{Z}$ is zero.

As we let the maps $C_k \rightarrow \Lambda$ range over all 1-cocycles, their images cover the kernel ${}_N\Lambda$ of the norm map, so that ψ restricts to 0 on ${}_N\Lambda$. Since ${}_N\Lambda$ is a pure submodule of Λ , we may lift ψ to a homomorphism $\tilde{\psi}: \Lambda \rightarrow \mathbb{Q}$ which vanishes on ${}_N\Lambda$. But the C_k -action on $\Lambda/{}_N\Lambda$ is trivial, so such a $\tilde{\psi}$ is automatically C_k -equivariant. Hence ψ is the image of $\tilde{\psi}$ under the map $H^0(C_k, \text{Hom}(\Lambda, \mathbb{Q})) \rightarrow H^0(C_k, \text{Hom}(\Lambda, \mathbb{Q}/\mathbb{Z}))$, and so $[\phi] = \delta(\psi) = 0$, as desired. \square

Having dealt with the case of $H^1(C_k, \Lambda)$, the corresponding properties of \mathfrak{B}_Λ are now straightforward to prove.

Proposition 2.2.2. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Write the characteristic (respectively minimal) polynomial of a generator as $\pm(t-1)^r P(t)$ with $P(1) > 0$ (respectively $\pm(t-1)^{r_0} P_0(t)$ with $P_0(1) > 0$). Then:*

- \mathfrak{B}_Λ is a finite group, with exponent dividing $P_0(1) \mid k$ and order dividing $P(1)$;
- the cup product pairing $H^1(C_k, \Lambda) \otimes H^1(C_k, \Lambda) \rightarrow H^2(C_k, \mathbb{Z}) \cong C_k^*$ descends to a perfect antisymmetric pairing on \mathfrak{B}_Λ .

Proof. Since \mathfrak{B}_Λ is by definition a quotient of $H^1(C_k, \Lambda)$, the first point follows immediately from Proposition 2.2.1. For the second part, we note that the given pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$ and the evaluation pairing $\Lambda^\vee \otimes \Lambda \rightarrow \mathbb{Z}$ are related by the associated map $\iota: \Lambda \hookrightarrow \Lambda^\vee$, in that we have a commuting diagram

$$\begin{array}{ccc} \Lambda \otimes \Lambda & \longrightarrow & \mathbb{Z} \\ \downarrow \iota \otimes 1 & & \parallel \\ \Lambda^\vee \otimes \Lambda & \longrightarrow & \mathbb{Z}. \end{array}$$

By naturality of cup product, we have a similar diagram

$$\begin{array}{ccc} H^1(C_k, \Lambda) \otimes H^1(C_k, \Lambda) & \longrightarrow & H^2(C_k, \mathbb{Z}) \\ \downarrow \iota_* \otimes 1 & & \parallel \\ H^1(C_k, \Lambda^\vee) \otimes H^1(C_k, \Lambda) & \longrightarrow & H^2(C_k, \mathbb{Z}) \end{array}$$

relating the induced cup product pairings on cohomology. But now $H^2(C_k, \mathbb{Z}) \cong C_k^*$ is canonically (Pontryagin) dual to C_k , and the bottom pairing is perfect by Proposition 2.2.1, so we identify the composite map $H^1(C_k, \Lambda) \xrightarrow{\iota_*} H^1(C_k, \Lambda^\vee) \cong \text{Hom}(H^1(C_k, \Lambda), C_k^*)$ as the map induced by the top cup product.

But now it follows completely formally that the left-kernel of the cup product $H^1(C_k, \Lambda) \otimes H^1(C_k, \Lambda) \rightarrow H^2(C_k, \mathbb{Z})$ is exactly the kernel of $\iota_*: H^1(C_k, \Lambda) \rightarrow H^1(C_k, \Lambda^\vee)$. Since the cup product pairing is antisymmetric, this is also the right-kernel, and so the cup product factors uniquely through $\mathfrak{B}_\Lambda \otimes \mathfrak{B}_\Lambda$ as an antisymmetric perfect pairing. \square

Remark 2.2.3. If the C_k action on Λ factors through some quotient C_l with $l \mid k$, then $H^1(C_k, \Lambda) = H^1(C_l, \Lambda)$ (since Λ is torsion-free) and \mathfrak{B}_Λ doesn't depend on whether we consider Λ with the action of C_k or of C_l .

2.3. Explicit descriptions of \mathfrak{B}_Λ and $H^1(C_k, \Lambda)$. For the purposes of computing examples, it is worth noting that all the quantities in Theorem 2.1.1 can be made quite explicit, in such a way that for low-dimensional lattices one can often find them simply by inspection. Of the quantities of interest, the only inexplicit ones are the lattice cohomology $H^1(C_k, \Lambda)$ and the group \mathfrak{B}_Λ , which we now describe in turn.

In order to understand $H^1(C_k, \Lambda)$, it will be useful for us to introduce a certain *separation group* associated to Λ , which measures the failure of Λ to decompose as the direct sum of its invariant sublattice and the kernel of the norm map.

Definition 2.3.1. Let Λ be a lattice endowed with an action by a cyclic group $C_k = \langle \sigma \rangle$. We write ${}_N\Lambda \leq \Lambda$ for, equivalently:

- the kernel of the norm map $1 + \sigma + \dots + \sigma^{k-1}$;
- the intersection of Λ with the largest invariant subspace of $\mathbb{Q} \otimes \Lambda$ with no non-trivial fixed vector;
- the smallest saturated sublattice of Λ containing $(\sigma - 1)\Lambda$;
- the orthogonal complement of Λ^{C_k} with respect to any *positive definite* C_k -invariant symmetric pairing.

Then ${}_N\Lambda \oplus \Lambda^{C_k}$ is a full-rank sublattice of Λ , and we define the *separation group* of Λ to be the finite group

$$\mathcal{T}_\Lambda := \Lambda / ({}_N\Lambda \oplus \Lambda^{C_k}).$$

Proposition 2.3.2. *Let Λ be a lattice endowed with an action by a cyclic group C_k . Write the characteristic polynomial of a generator σ as $\pm(t-1)^{\text{rk}(\Lambda^{C_k})}P(t)$ with $P(1) > 0$. Then*

$$|H^1(C_k, \Lambda)| = \frac{P(1)}{|\mathcal{T}_\Lambda|}.$$

Proof. From the discussion in Proposition 2.2.1, we have an exact sequence

$$0 \rightarrow \Lambda^{C_k} \rightarrow \Lambda/_N \Lambda \rightarrow H^1(C_k, {}_N \Lambda) \rightarrow H^1(C_k, \Lambda) \rightarrow 0$$

and by definition \mathcal{T}_Λ is the cokernel of the left-hand arrow. In particular, we have

$$|\mathcal{T}_\Lambda| \cdot |H^1(C_k, \Lambda)| = |H^1(C_k, {}_N \Lambda)| = P(1),$$

as desired. \square

Corollary 2.3.3. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing. Write the characteristic (respectively minimal) polynomial of a generator as $\pm(t-1)^r P(t)$ with $P(1) > 0$ (respectively $\pm(t-1)^{r_0} P_0(t)$). Then \mathcal{T}_Λ is a finite abelian group, with exponent dividing $P_0(1) \mid k$ and order dividing $P(1)$.*

Proof. The proof of Proposition 2.2.1 showed that $H^1(C_k, {}_N \Lambda)$ is a finite abelian group of exponent dividing $P_0(1) \mid k$ and order exactly $P(1)$. The proof of Proposition 2.3.2 showed that \mathcal{T}_Λ is a subgroup of $H^1(C_k, {}_N \Lambda)$, so we are done. \square

In the formula in Proposition 2.3.2, it is worth noting that the quantity $P(1)$ is also quite straightforward to understand in terms of the order of a generator acting on the various irreducible summands of $\mathbb{Q} \otimes \Lambda$.

Lemma 2.3.4. *Let Λ be a lattice endowed with an action by a cyclic group C_k . Write the characteristic polynomial (respectively minimal polynomial) of a generator σ as $\pm(t-1)^r P(t)$ with $P(1) > 0$ (respectively $\pm(t-1)^{r_0} P_0(t)$). Then:*

- $P(1) = \prod_{q^s} q^{a_{q^s}}$, where the product is taken over prime powers $q^s > 1$, and a_m denotes the multiplicity of a fixed primitive m th root of unity as an eigenvalue of σ ; and
- $P_0(1) = \prod_{q^s} q^{b_{q^s}}$, where $b_m = 0$ or 1 according as $a_m = 0$ or $a_m > 0$.

Proof. The characteristic (respectively minimal) polynomial of σ factorises as a product $\prod_m \Phi_m(t)^{a_m}$ (respectively $\prod_m \Phi_m(t)^{b_m}$) of cyclotomic polynomials, so that $P(1) = \prod_{m>1} \Phi_m(1)^{a_m}$ (respectively $P_0(1) = \prod_{m>1} \Phi_m(1)^{b_m}$). Thus we are done by the following lemma. \square

Lemma 2.3.5. $\Phi_k(1) = q$ if $k = q^s$ is a prime power; $\Phi_k(1) = 1$ for all other $k \neq 1$.

Proof. This follows by substituting $X = 1$ into the formula $\frac{X^k - 1}{X - 1} = \prod_{1 \neq j \mid k} \Phi_j(X)$ and using induction on k . \square

Our explicit description of \mathfrak{B}_Λ is a little more complicated, but can nonetheless be usually worked out straightforwardly in practice.

Lemma 2.3.6. *Let Λ be a lattice endowed with an action by a cyclic group $C_k = \langle \sigma \rangle$ and a non-degenerate C_k -equivariant symmetric pairing. Then*

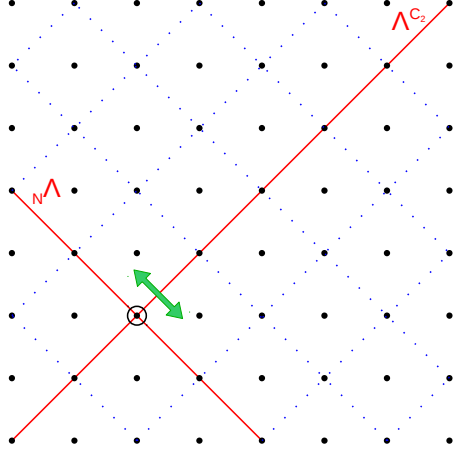
$$\mathfrak{B}_\Lambda \cong \frac{{}_N \Lambda}{(\sigma - 1)\Lambda^\vee \cap {}_N \Lambda},$$

where the intersection is taken inside Λ^\vee via the embedding $\Lambda \hookrightarrow \Lambda^\vee$ induced from the pairing.

Proof. From the usual description $H^1(C_k, \Lambda) \cong {}_N \Lambda / (\sigma - 1)\Lambda$ and the definition of \mathfrak{B}_Λ , it follows that $\mathfrak{B}_\Lambda = ({}_N \Lambda + (\sigma - 1)\Lambda^\vee) / (\sigma - 1)\Lambda^\vee \cong {}_N \Lambda / ((\sigma - 1)\Lambda^\vee \cap {}_N \Lambda)$. \square

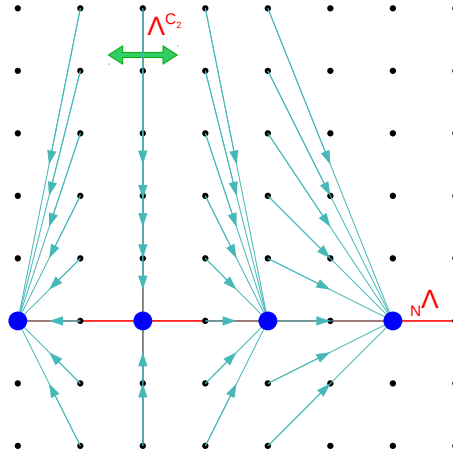
Let us conclude this subsection by giving two examples, illustrating how one can work out these examples in low-dimensional examples.

Example 2.3.7. Let $\Lambda = \mathbb{Z}^2$ endowed with the action of $C_2 = \langle \sigma \rangle$ where the generator σ acts by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, the reflection in the $x = y$ line. The picture is the following:



Here the action of σ is indicated by the diagonal arrow. The invariant subspace Λ^{C_2} (resp. the kernel ${}_N\Lambda$ of the norm map) is the line $x = y$ (resp. $x = -y$); these are indicated by the bold lines. Even though the ambient \mathbb{R} -vector space decomposes as a sum of these subspaces, Λ does not: the dotted lines serve to identify the lattice sum ${}_N\Lambda \oplus \Lambda^{C_2}$, which is clearly index 2 in Λ . Hence $\mathcal{T}_\Lambda \simeq C_2$ and $H^1(C_2, \Lambda) = 1$ by Proposition 2.3.2.

Example 2.3.8. Consider $\Lambda = \mathbb{Z}^2$ endowed with the standard inner product and the action of $C_2 = \langle \sigma \rangle$ where the generator σ acts by $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, the reflection in the y -axis. The picture is the following:



Here the action of σ is indicated by the horizontal double-headed arrow. We have $\Lambda^\vee = \Lambda$, the kernel ${}_N\Lambda$ of the norm map (intersection of Λ with the sum of the eigenspaces with eigenvalue $\neq 1$) is the x -axis, and $(1-\sigma)$ is twice the projection onto the x -axis, as indicated by the single-headed arrows. The larger dots on the x -axis serve to identify the image of this map, and hence the group $\mathfrak{B}_\Lambda = {}_N\Lambda / ({}_N\Lambda \cap (1-\sigma)\Lambda^\vee)$ is visibly C_2 .

2.4. Growth in towers (up to squares). As well as the quantity $|(\Lambda^\vee/\Lambda)^{C_k}|$ associated to a lattice Λ with C_k -action and C_k -invariant non-degenerate pairing, we will be interested in the quantities

$$|(\Lambda^\vee/e\Lambda)^{fC_k}|$$

for varying $e, f \in \mathbb{N}$. These can be identified with the quantities $|(\Lambda_{e,f}^\vee / \Lambda_{e,f})^{C_{\text{hcf}(f,k)}}|$ where $\Lambda_{e,f}$ is the lattice formed by restricting the action to $fC_k \leq C_k$ and scaling the pairing by a factor of e , and hence which, when Λ is the character lattice of the toric part of the Raynaud parametrisation of a semistable principally polarised abelian variety, computes the Tamagawa number over finite extensions of ramification degree e and residue class degree f . Corollary 2.1.3 completely resolves the problem of dependence on e , so we will now focus on the dependence on f . Aside from a few facile observations (e.g. that $|(\Lambda^\vee / e\Lambda)^{fC_k}|$ depends only on $\text{hcf}(f, k)$), we will only be able to satisfactorily control the f -dependence up to squares, but this is nonetheless sufficient for our parity conjecture applications.

Here is the main abstract result affording us control of orders of groups up to squares.

Theorem 2.4.1. *Let A be a finite abelian group endowed with a perfect pairing $\langle \cdot, \cdot \rangle: A \otimes A \rightarrow \mathbb{Q}/\mathbb{Z}$. Let \sim denote equality up to rational squares.*

- (1) *If $\langle \cdot, \cdot \rangle$ is antisymmetric, then $|A|$ is either a square or twice a square; it is square if the pairing is alternating. Moreover,*

$$|A[e]| \sim \begin{cases} |A| & \text{if } 2 \mid e, \\ 1 & \text{if } 2 \nmid e. \end{cases}$$

- (2) *If A carries an action by a cyclic group C_k and $\langle \cdot, \cdot \rangle$ is symmetric and C_k -invariant, then*

$$|A^{fC_k}| \sim \begin{cases} |A^{C_k}| & \text{if } 2 \nmid f, \\ |A| & \text{if } 2 \mid f. \end{cases}$$

Before we prove this theorem, let us give the main application to the Tamagawa numbers.

Theorem 2.4.2. *Let Λ be a lattice endowed with an action by a cyclic group C_k and non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Then for all $e, f \in \mathbb{N}$*

$$\left| (\Lambda^\vee / e\Lambda)^{fC_k} \right| \sim \begin{cases} |(\Lambda^\vee / \Lambda)^{C_k}| \cdot e^{\text{rk}(\Lambda^{C_k})} & \text{if } 2 \nmid e, 2 \nmid f, \\ |(\Lambda^\vee / \Lambda)^{C_k}| \cdot |\mathfrak{B}_\Lambda| \cdot e^{\text{rk}(\Lambda^{C_k})} & \text{if } 2 \mid e, 2 \nmid f, \\ |(\Lambda^\vee / \Lambda)| \cdot e^{\text{rk}(\Lambda)} & \text{if } 2 \mid f. \end{cases}$$

Proof. Since the inclusion $\Lambda \hookrightarrow \Lambda^\vee$ becomes an isomorphism when tensored with \mathbb{Q} , Λ^\vee carries a unique C_k -invariant symmetric \mathbb{Q} -valued pairing extending the \mathbb{Z} -valued pairing on Λ . We let $\langle \cdot, \cdot \rangle: \Lambda^\vee \otimes \Lambda^\vee \rightarrow \mathbb{Q}/e\mathbb{Z}$ denote the reduction of this pairing mod $e\mathbb{Z}$. It is then easy to see that the left- and right-kernels of the pairing are both $e\Lambda \leq \Lambda^\vee$, so that $\langle \cdot, \cdot \rangle$ descends to a C_k -invariant symmetric perfect pairing on $\Lambda^\vee / e\Lambda$. Hence by Theorem 2.4.1 we have

$$|(\Lambda^\vee / e\Lambda)^{fC_k}| \sim \begin{cases} |(\Lambda^\vee / e\Lambda)^{C_k}| & \text{if } 2 \nmid f, \\ |(\Lambda^\vee / e\Lambda)| & \text{if } 2 \mid f. \end{cases}$$

Since $|(\Lambda^\vee / e\Lambda)| = |(\Lambda^\vee / \Lambda)| \cdot e^{\text{rk}(\Lambda)}$, we are done when f is even, and when f is odd we may reduce to the case that $f = 1$.

For this case, we recall from Proposition 2.2.2 that \mathfrak{B}_Λ carries a perfect anti-symmetric pairing with values in $C_k^* \simeq \mathbb{Z}/k\mathbb{Z}$. Hence by Theorem 2.4.1 again

$$|\mathfrak{B}_\Lambda[e]| \sim \begin{cases} |\mathfrak{B}_\Lambda| & \text{if } 2 \mid e, \\ 1 & \text{if } 2 \nmid e. \end{cases}$$

Combining this with Corollary 2.1.3 yields the desired result. \square

Corollary 2.4.3. *Let Λ be a lattice endowed with an action by a cyclic group C_k and a non-degenerate C_k -invariant symmetric pairing $\Lambda \otimes \Lambda \rightarrow \mathbb{Z}$. Let $\Lambda_{e,f}$ for $e, f \in \mathbb{N}$ denote the lattice formed by restricting the action to $fC_k \leq C_k$ and scaling the pairing by a factor of e . Then*

$$|\mathfrak{B}_{\Lambda_{e,f}}| \sim \begin{cases} |\mathfrak{B}_\Lambda| & \text{if } 2 \nmid f, 2 \nmid e, \\ 1 & \text{else.} \end{cases}$$

Proof. From Theorem 2.4.2 applied to the lattice $\Lambda_{e,f}$ it follows that

$$|\mathfrak{B}_{\Lambda_{e,f}}| \sim \frac{|(\Lambda^\vee/4e\Lambda)^{fC_k}|}{|(\Lambda^\vee/e\Lambda)^{fC_k}|}.$$

Calculating the numerator and denominator up to squares using Theorem 2.4.2 again yields the desired result. \square

Proof of Theorem 2.4.1. (1) The fact about $|A|$ is standard. To deduce the description of $|A[e]|$ up to squares, consider the \mathbb{Q}/\mathbb{Z} -valued pairing $\langle x, y \rangle_e = e\langle x, y \rangle$ on A – it is clearly antisymmetric and its left- and right-kernels are $A[e]$, so it descends to a perfect antisymmetric pairing on $A/A[e]$, which is even alternating when e is even.

If e is odd, then this tells us that $|A[e]|$, like $|A|$, is either a square or twice a square – it must be then a square since it is odd. If instead e is even, then the alternating pairing on $A/A[e]$ ensures that the sizes of $A[e]$ and A agree up to squares.

(2) If f is even, let σ be a generator of C_k , $\Theta = \sigma^{f/2} - \sigma^{-f/2}$, and consider the pairing $\langle x, y \rangle_\Theta = \langle \Theta x, y \rangle$ on A . It is easy to check (as $\langle \sigma^{f/2}x, x \rangle = \langle x, \sigma^{-f/2}x \rangle$) that $\langle \cdot, \cdot \rangle_\Theta$ is alternating. Moreover, its left- and right-kernels are both $A[\Theta] = A^{fC_k}$, so descends to a perfect alternating pairing on A/A^{fC_k} . Hence $|A^{fC_k}| \sim |A|$ as claimed.

If instead f is odd, let $\Theta = (\sigma - \sigma^{-1})(\sigma^{(f-1)/2} + \dots + \sigma^{(1-f)/2})$. By the same argument as above, $A[\Theta] \leq A$ has square index, so that $A^{2C_k} \leq A[\Theta]$ has square index too. But also we have $A[\Theta] = A^{fC_k} + A^{2C_k}$: the right-to-left containment is obvious, and conversely $(\sigma + 1)A[\Theta] \leq A^{fC_k}$ and $(\sigma^{f-1} + \dots + 1)A[\Theta] \leq A^{2C_k}$, so that $A[\Theta] \leq (\sigma + 1)A[\Theta] + (\sigma^{f-1} + \dots + 1)A[\Theta] \leq A^{fC_k} + A^{2C_k}$, as desired.

Combining these, we have by the second isomorphism theorem for groups that

$$\frac{A^{fC_k}}{A^{C_k}} = \frac{A^{fC_k}}{A^{fC_k} \cap A^{2C_k}} \cong \frac{A^{fC_k} + A^{2C_k}}{A^{2C_k}} = \frac{A[\Theta]}{A^{2C_k}}$$

which has square order, as desired. \square

2.5. Examples. In preparation for our main result classifying low-dimensional lattices with pairings, let us give some specific examples of lattices Λ that arise in practice, and compute their invariants.

As a most basic example of what can occur, we have the following immediate consequence of Shapiro's lemma.

Lemma 2.5.1. *Suppose that X is a finite C_k -set and let $\Lambda \simeq \mathbb{Z}[X]$ be the associated permutation representation, equipped with any C_k -invariant symmetric pairing. Then $H^1(C_k, \Lambda)$ and \mathfrak{B}_Λ are trivial. $(\Lambda^\vee)^{C_k}$ is the lattice of C_k -invariant functions on X , and Λ^{C_k} is the rank $|C_k \backslash X|$ sublattice of $\mathbb{Z}[X]$ generated by the formal sums of the elements in each C_k -orbit. We have*

$$|(\Lambda^\vee / e\Lambda)^{C_k}| = |((\Lambda^\vee)^{C_k} / \Lambda^{C_k})| \cdot e^{|C_k \backslash X|}.$$

Our approach to classifying the low-dimensional C_k -lattices Λ will proceed first by dividing into cases corresponding to the irreducible factors of the rational C_k -representation $\mathbb{Q} \otimes \Lambda$; these irreducible factors are of the form $\mathbb{Q}(\zeta_l)$ for $l \mid k$, where a generator of C_k acts by multiplication by the primitive l th root of unity ζ_l . Thus it will be useful for us to completely understand the case when $\mathbb{Q} \otimes \Lambda \simeq \mathbb{Q}(\zeta_l)$ is irreducible.

Lemma 2.5.2. *Let Λ be a lattice representation of C_k ($k > 1$) such that $\mathbb{Q} \otimes \Lambda$ is the unique faithful irreducible rational representation of C_k . Fix a generator $\sigma \in C_k$.*

(i) $\Lambda \simeq \mathfrak{a}$ for some fractional ideal \mathfrak{a} of $\mathbb{Q}(\zeta_k)$, where σ acts on $\mathbb{Q}(\zeta_k)$ by multiplication by a primitive k -th root of unity ζ_k . Two such lattices are isomorphic as $\mathbb{Z}[C_k]$ -representations if and only if the corresponding fractional ideals are equivalent in the ideal class group $\mathbf{Cl}_{\mathbb{Q}(\zeta_k)}$.

(ii) The non-degenerate C_k -invariant \mathbb{Q} -valued symmetric pairings on $\Lambda \simeq \mathfrak{a}$ are given by

$$\langle x, y \rangle = \text{tr}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\omega x \bar{y})$$

for non-zero $\omega \in \mathbb{Q}(\zeta_k)^+$. This pairing is \mathbb{Z} -valued iff $\omega \in (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_k)^{-1}$, where $\mathfrak{D}_k^{-1} = \mathfrak{D}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}^{-1}$ is the inverse different ideal², and the canonical isomorphism $\mathbb{Q} \otimes \Lambda \xrightarrow{\sim} \mathbb{Q} \otimes \Lambda^\vee$ embeds Λ^\vee in $\mathbb{Q}(\zeta_k)$ as the fractional ideal $(\omega\bar{\mathfrak{a}}\mathfrak{D}_k)^{-1}$.

(iii) Suppose $\Lambda \simeq \mathfrak{a}$ as above is endowed with the non-degenerate C_k -invariant symmetric pairing defined by some $\omega \in (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_k)^{-1} \cap (\mathbb{Q}(\zeta_k)^+ \setminus \{0\})$. Then $H^1(C_k, \Lambda) \simeq \mathbb{Z}/q\mathbb{Z}$ if $k = q^s$ is a prime power, and is trivial otherwise. \mathfrak{B}_Λ is trivial unless $k = 2^s$ and $N(\omega\bar{\mathfrak{a}}\mathfrak{a}\mathfrak{D}_k)$ is odd, in which case $\mathfrak{B}_\Lambda \simeq \mathbb{Z}/2\mathbb{Z}$. In particular

$$\left| \left(\frac{\Lambda^\vee}{e\Lambda} \right)^{C_k} \right| = \begin{cases} q & \text{if } k = q^s, q \text{ an odd prime,} \\ 2 & \text{if } k = 2^s \text{ and } N(\omega\bar{\mathfrak{a}}\mathfrak{a}\mathfrak{D}_k) \text{ is even,} \\ 1 & \text{otherwise.} \end{cases}$$

Proof. (i) $\mathbb{Q} \otimes \Lambda \simeq \mathbb{Q}(\zeta_k)$, this being the unique faithful irreducible rational representation of C_k . The image of Λ in $\mathbb{Q}(\zeta_k)$ is then a finitely-generated $\mathbb{Z}[\zeta_k]$ -submodule, and hence a fractional ideal \mathfrak{a} of $\mathbb{Q}(\zeta_k)$. Finally, two such lattices are isomorphic as $\mathbb{Z}[C_k]$ -representations if and only if the corresponding fractional ideals are isomorphic as $\mathbb{Z}[\zeta_k]$ -modules, which is equivalent to them having the same class in $\mathbf{Cl}_{\mathbb{Q}(\zeta_k)}$ (the only possible isomorphisms are scaling by $x \in \mathbb{Q}(\zeta_k)$).

²i.e. $\mathfrak{D}_k^{-1} = \{z \in \mathbb{Z}[\zeta_k] \mid \forall w \in \mathbb{Z}[\zeta_k] : \text{tr}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(zw) \in \mathbb{Z}\}$

(ii) Let Σ denote the space of all C_k -invariant \mathbb{Q} -valued symmetric bilinear forms on $\mathbb{Q}(\zeta_k)$. C_k -invariance implies that bilinear forms are determined by the \mathbb{Q} -linear map $z \mapsto (1, z)$. Moreover, C_k -invariance and symmetry give that $(1, z) = (1, \bar{z})$ for all z , so $(1, z) = (1, \text{Re}(z))$ and so the bilinear forms are determined by the restriction of $z \mapsto (1, z)$ to $\mathbb{Q}(\zeta_k)^+$. Thus Σ injects \mathbb{Q} -linearly into $\text{Hom}_{\mathbb{Q}}(\mathbb{Q}(\zeta_k)^+, \mathbb{Q})$. In particular, $\dim \Sigma \leq [\mathbb{Q}(\zeta_k)^+ : \mathbb{Q}]$.

Conversely, the assignment of the form $(x, y) = \text{tr}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\omega x \bar{y})$ to $\omega \in \mathbb{Q}(\zeta_k)^+$ provides a \mathbb{Q} -linear injection $\mathbb{Q}(\zeta_k)^+ \hookrightarrow \Sigma$. By dimension considerations, it must be a linear isomorphism. Thus all C_k -equivariant \mathbb{Q} -valued symmetric bilinear forms must be of this form. The only degenerate one is when $\omega = 0$.

With respect to this pairing, some $x \in \mathbb{Q} \otimes \Lambda = \mathbb{Q}(\zeta_k)$ lies in Λ^\vee exactly when $\text{tr}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\omega x \bar{a}) \leq \mathbb{Z}$, which occurs precisely when $\omega x \bar{a} \leq \mathfrak{D}_k^{-1}$. Hence $\Lambda^\vee = (\omega \bar{a} \mathfrak{D}_k)^{-1}$ as a submodule of $\mathbb{Q}(\zeta_k)$. The pairing is then integral on Λ if and only if $\Lambda \leq \Lambda^\vee$, which occurs if and only if $\omega \in (\bar{a} \mathfrak{D}_k)^{-1}$, as desired.

(iii) The characteristic polynomial of σ is the cyclotomic polynomial Φ_k . Hence σ has no fixed points, so that ${}_N\Lambda = \Lambda$ and $|\text{H}^1(C_k, \Lambda)| = \Phi_k(1)$ by Proposition 2.3.2. The computation of $\Phi_k(1)$ in Lemma 2.3.5 gives the description of $\text{H}^1(C_k, \Lambda)$.

As for \mathfrak{B}_Λ , it is a quotient of $\text{H}^1(C_k, \Lambda)$ and admits a perfect antisymmetric pairing, so its order divides $\Phi_k(1)$ and also is either a square or twice a square. Hence it is trivial, unless $k = 2^s$, in which case it is either trivial or $\mathbb{Z}/2\mathbb{Z}$.

In the case that $k = 2^s$, we have by Theorem 2.1.1 that $|(\Lambda^\vee/\Lambda)^{C_k}| \cdot |\mathfrak{B}_\Lambda| = 2$, so that exactly one of $(\Lambda^\vee/\Lambda)^{C_k}$ and \mathfrak{B}_Λ is trivial, and the other is $\mathbb{Z}/2\mathbb{Z}$. Now if the quantity $|(\Lambda^\vee/\Lambda)| = N(\omega \bar{a} \mathfrak{D}_k)$ is odd, so too is $|(\Lambda^\vee/\Lambda)^{C_k}|$ and hence $\mathfrak{B}_\Lambda \simeq \mathbb{Z}/2\mathbb{Z}$. On the other hand, if the quantity is even, then $(\Lambda^\vee/\Lambda)[2]$ is a non-trivial \mathbb{F}_2 -vector space with an action by a 2-power cyclic group, and hence has a non-trivial fixed vector by the orbit-stabiliser theorem. Hence $|(\Lambda^\vee/\Lambda)^{C_k}| > 1$ and \mathfrak{B}_Λ is trivial.

The final formula follows from Theorem 2.1.1 since $(\Lambda^\vee)^{C_k} = 1$. \square

Remark 2.5.3. The different ideal \mathfrak{D}_k is explicitly given by

$$\mathfrak{D}_k = \mathfrak{D}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}} = k \cdot \prod_{q|k \text{ prime}} (\zeta_q - 1)^{-1}.$$

To see this, first recall that as the ring of integers of $\mathbb{Q}(\zeta_k)$ is $\mathbb{Z}[\zeta_k]$, its different is generated by $\Phi'_n(\zeta_k)$ (see e.g. [16] remark on p 96). The cyclotomic polynomial can be expressed as

$$\Phi_k(X) = \prod_{t|k} (X^{k/t} - 1)^{\mu(t)}$$

where μ is the Möbius μ -function, and hence, by l'Hôpital's rule

$$\frac{\Phi'_k(\zeta_k)}{k\zeta_k^{k-1}} = \prod_{1 \neq t|k} (\zeta_k^{k/t} - 1)^{\mu(t)} = \text{unit} \times \prod_{q|k \text{ prime}} (\zeta_q - 1)^{-1},$$

where for the second equality we have used that fact that $\mu(t) = 0$ for non-squarefree t and that $(\zeta_k - 1)$ is a unit when k is not a prime power. (The latter result follows from the identity $N_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(1 - \zeta_k) = \prod_{0 < s < k, (s, k) = 1} (1 - \zeta_k^s) = \Phi_k(1)$, which is 1 by Lemma 2.3.5, so that $1 - \zeta_k$ is a unit.) The claim follows.

2.6. Classification of rank 1 and 2 lattices. To conclude this section, let us now give the promised classification of lattices in dimensions 1 and 2, along with their invariants. Since the quantity $(\Lambda^\vee/\Lambda)^{C_k}$ depends only on Λ^\vee as an overlattice

of Λ , we will in fact only classify the possible lattice-pairs $\Lambda \leq \Lambda^\vee$ which can arise from a pairing on Λ , and not the pairings themselves.

The rank 1 case is essentially trivial, but we record it here for completeness.

Lemma 2.6.1. *Let Λ be a rank 1 lattice representation of $C_k = \langle \sigma \rangle$ endowed with a non-degenerate C_k -invariant symmetric \mathbb{Z} -valued pairing. Embed $\Lambda^\vee \hookrightarrow \mathbb{Q} \otimes \Lambda$ by inverting the canonical isomorphism $\mathbb{Q} \otimes \Lambda \xrightarrow{\sim} \mathbb{Q} \otimes \Lambda^\vee$. Then, up to $\mathbb{Z}[C_k]$ -isomorphism, the pair of lattices $\Lambda \leq \Lambda^\vee$ is one of the following:*

Type	Λ	Λ^\vee	σ	$H^1(C_k, \Lambda)$	\mathfrak{B}_Λ	$ (\Lambda^\vee/\Lambda)^{C_k} $
$[1 : n]$	\mathbb{Z}	$\frac{1}{n}\mathbb{Z}$	+1	1	1	n
$[2 : n]$	\mathbb{Z}	$\frac{1}{n}\mathbb{Z}$	-1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	1 $(n \text{ odd})$
					1	2 $(n \text{ even})$

The parameter n is a positive integer. All of the types arise from integral representations with a corresponding symmetric pairing and no two are isomorphic. The associated groups $H^1(C_k, \Lambda)$, \mathfrak{B}_Λ and $(\Lambda^\vee/\Lambda)^{C_k}$ are as described in the table.

Proof. As $\Lambda \simeq \mathbb{Z}$ as an abelian group, the automorphism σ is either multiplication by 1 or by -1 . The pairing can be any \mathbb{Z} -valued non-zero pairing, so, in particular, Λ^\vee can be any finite overlattice of Λ . The invariants $H^1(C_k, \Lambda)$, \mathfrak{B}_Λ and $|(\Lambda/\Lambda^\vee)^{C_k}|$ are elementary to compute directly from the definitions. \square

Theorem 2.6.2. *Let Λ be a rank 2 lattice representation of $C_k = \langle \sigma \rangle$ endowed with a non-degenerate C_k -invariant symmetric \mathbb{Z} -valued pairing. Embed $\Lambda^\vee \hookrightarrow \mathbb{Q} \otimes \Lambda$ by inverting the canonical isomorphism $\mathbb{Q} \otimes \Lambda \xrightarrow{\sim} \mathbb{Q} \otimes \Lambda^\vee$. Then, up to $\mathbb{Z}[C_k]$ -isomorphism, the pair of lattices $\Lambda \leq \Lambda^\vee$ is one of the following:*

Type	Λ	Λ^\vee	σ	$H^1(C_k, \Lambda)$	\mathfrak{B}_Λ	$ (\Lambda^\vee/\Lambda)^{C_k} $
$[1.1 : m, n]$	$\mathbb{Z}^{\oplus 2}$	$\frac{1}{m}\mathbb{Z} \oplus \frac{1}{n}\mathbb{Z}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	1	mn
$[1.2_A : m, n]$	$\mathbb{Z}^{\oplus 2}$	$\frac{1}{m}\mathbb{Z} \oplus \frac{1}{n}\mathbb{Z}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	m $(n \text{ odd})$
					1	$2m$ $(n \text{ even})$
$[1.2_B : m, n]$	$\mathbb{Z}^{\oplus 2} + \langle \frac{1}{2}, \frac{1}{2} \rangle$	$\frac{1}{m}\mathbb{Z} \oplus \frac{1}{n}\mathbb{Z} + \langle \frac{1}{2m}, \frac{1}{2n} \rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	1	1	$ m+n $
$[2.2 : m, n]$	$\mathbb{Z}^{\oplus 2}$	$\frac{1}{m}\mathbb{Z} \oplus \frac{1}{n}\mathbb{Z}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	1 $(m, n \text{ odd})$
					$\mathbb{Z}/2\mathbb{Z}$	2 $(m, n \text{ odd/even})$
					1	4 $(m, n \text{ even})$
$[3 : n]$	$\mathbb{Z}[\zeta_3]$	$\frac{\zeta_3-1}{3n}\mathbb{Z}[\zeta_3]$	$\cdot \zeta_3$	$\mathbb{Z}/3\mathbb{Z}$	1	3
$[4 : n]$	$\mathbb{Z}[i]$	$\frac{1}{n}\mathbb{Z}[i]$	$\cdot i$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	1 $(n \text{ odd})$
					1	2 $(n \text{ even})$
$[6 : n]$	$\mathbb{Z}[\zeta_3]$	$\frac{\zeta_3-1}{3n}\mathbb{Z}[\zeta_3]$	$\cdot \zeta_6$	1	1	1

In all types save $[1.2_B : m, n]$ the parameters m and n are positive integers. In type $[1.2_B : m, n]$ the parameters m and n are positive integers of the same parity.

Types $[1.1 : m, n]$ and $[1.1 : m', n']$ are isomorphic if and only if $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}$, and similarly for type $[2.2 : m, n]$; no other pairs are isomorphic.

The associated groups $H^1(C_k, \Lambda)$, \mathfrak{B}_Λ and $(\Lambda^\vee/\Lambda)^{C_k}$ are as described in the table. All of the above types arise from integral representations with a corresponding symmetric pairing.

Remark 2.6.3. (i) Our notion of “type” refers to an isomorphism class of pairs $\Lambda \leq \Lambda^\vee$ of equal-rank lattices with C_k -action which can be induced by some (unspecified) C_k -equivariant pairing on Λ . For most types, this pairing is essentially determined by the lattice-pair, with the exception of types $[1.1 : m, n]$ and $[2.2 : m, n]$ (where for example the pairings giving rise to type $[1.1 : 1, 1]$ are parametrised by symmetric unimodular integer matrices up to equivalence).

(ii) The first digits in the types give the decomposition of the rational representation $\mathbb{Q} \otimes \Lambda$ into irreducibles $(\mathbb{Q}(\zeta_l))$ for $l \in \mathbb{N}$, where σ acts by multiplication by ζ_l . For instance, 1.2 refers to the decomposition $\mathbb{Q} \otimes \Lambda \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta_2)$.

(iii) In types $[1.1 : m, n]$, $[1.2_A : m, n]$, $[1.2_B : m, n]$ and $[2.2 : m, n]$, the descriptions of Λ , Λ^\vee and σ are, of course, written with respect to the same basis.

(iv) Note that to obtain $|(\Lambda^\vee/e\Lambda)^{C_k}|$ one simply needs to scale the parameters m, n by e , as this will just change Λ^\vee to $\frac{1}{e}\Lambda^\vee$.

Proof. Consider first $V = \mathbb{Q} \otimes \Lambda$, which is a 2-dimensional rational representation of a cyclic group. By complete reducibility of such representations, there are six possibilities for V : $\mathbb{Q}^{\oplus 2}$; $\mathbb{Q} \oplus \mathbb{Q}(\zeta_2)$; $\mathbb{Q}(\zeta_2)^{\oplus 2}$; $\mathbb{Q}(\zeta_3)$; $\mathbb{Q}(\zeta_4)$; and $\mathbb{Q}(\zeta_6)$, where on $\mathbb{Q}(\zeta_l)$ the generator σ acts by multiplication by ζ_l . The latter three cases are covered by Lemma 2.5.2, which gives the classification in these cases (types $[3 : n]$, $[4 : n]$ and $[6 : n]$ respectively). Note that the parameter ω defining the pairing is $\pm n$ in types $[3 : n]$ and $[6 : n]$, but $\pm n/2$ in type $[4 : n]$.

When $V \simeq \mathbb{Q}^{\oplus 2}$, the actions on Λ and Λ^\vee are trivial, so by a Smith normal form argument we may put Λ and Λ^\vee jointly in the form of type $[1.1 : m, n]$. The computation of the invariants is trivial in this case.

When $V \simeq \mathbb{Q}(\zeta_2)^{\oplus 2}$, the generator σ acts on both Λ and Λ^\vee by -1 . The same argument as above puts Λ and Λ^\vee jointly in the form of type $[2.2 : m, n]$. To compute the invariants, we just note that the pair $\Lambda \leq \Lambda^\vee$ is the direct sum of two rank 1 pairs of type $[2 : -]$, and that all the invariants behave multiplicatively under direct sums.

Finally, when $V \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta_2)$ there are two possibilities for Λ , depending on whether it is the split or the unique non-split extension of \mathbb{Z} by $\mathbb{Z}[\zeta_2]$. When $\Lambda \simeq \mathbb{Z} \oplus \mathbb{Z}[\zeta_2]$ splits, the decomposition is necessarily orthogonal for any C_k -invariant pairing, and hence Λ is an orthogonal direct sum of lattices of type $[1 : m]$ and $[2 : n]$, which is type $[1.2_A : m, n]$. The invariants are easily calculated by multiplicativity in orthogonal direct sums.

Finally, if Λ is the non-split extension of \mathbb{Z} by $\mathbb{Z}[\zeta_2]$, then it is isomorphic to the lattice in type $[1.2_B : -]$. Since the pairing must restrict to an integer-valued pairing on $\mathbb{Z}^{\oplus 2}$, it must be given by a matrix $\begin{pmatrix} m_0 & 0 \\ 0 & n_0 \end{pmatrix}$ with $m_0, n_0 \in \mathbb{Z}$ by the preceding case. The requirement that the pairing is integer-valued on Λ is equivalent to $m_0 = 2m$ and $n_0 = 2n$ with m and n integers of the same parity — this yields the dual lattice claimed. Finally, since Λ is the permutation representation corresponding to the translation action of C_k on C_2 , the invariants were calculated in Lemma 2.5.1. \square

3. TAMAGAWA NUMBERS OF SEMISTABLE ABELIAN VARIETIES

We now turn to the study of the behaviour of Tamagawa numbers of semistable abelian varieties in finite extensions of p -adic fields. Raynaud's parametrisation [13], [7]§9–10 allows us to translate this into a question about lattice quotients of the type investigated in §2. For the convenience of the reader, we will phrase the results in a way that does not require familiarity with the preceding section, except for the willingness to use the groups \mathfrak{B} and \mathcal{T} as black boxes.

In §3.1 we briefly review the theory of Tamagawa numbers of semistable abelian varieties and introduce the main notation. Our main results on Tamagawa numbers are contained in §3.2, followed by a classification of their behaviour for abelian varieties of toric dimension 2 in §3.3. Finally, we turn to abelian varieties over number fields and the p -parity conjecture in §3.4.

3.1. Character group $\Lambda_{A/K}$. Here we briefly review the theory of Tamagawa numbers of semistable abelian varieties. We only give a minimalistic description, and refer to [3] §3.5.1 for a more detailed overview, and the precise references therein for the proofs.

Notation 3.1.1. Let K/\mathbb{Q}_p be a finite extension, A/K a semistable principally polarised abelian variety, and K'/K an unramified extension over which A acquires split semistable reduction. Let T be the torus part of the Raynaud parametrisation of A/K' and $\Lambda_{A/K}$ its character group. This is a finite free \mathbb{Z} -module with an action of $\text{Gal}(K'/K)$. The monodromy pairing together with the principal polarisation give a non-degenerate symmetric $\text{Gal}(K'/K)$ -invariant pairing

$$(\cdot, \cdot) : \Lambda_{A/K} \times \Lambda_{A/K} \rightarrow \mathbb{Z}.$$

The pairing gives a natural embedding $\Lambda_{A/K} \subseteq \Lambda_{A/K}^\vee$.

We will write $\text{Fr} \in \text{Gal}(K^{nr}/K)$ for the Frobenius element, i.e. the element that acts as the Frobenius automorphism on the residue field. Its action on $\Lambda_{A/K}$ factors through the quotient $\text{Gal}(K'/K)$, so we will occasionally identify Fr with its image in the latter group.

Remark 3.1.2. The group scheme of connected components of the special fibre of the Néron model of A/\mathcal{O}_K is isomorphic to $\Lambda_{A/K}^\vee/\Lambda_{A/K}$, as groups with $\text{Gal}(K^{nr}/K)$ -action, and the local Tamagawa number is $c_{A/K} = \left| \left(\frac{\Lambda_{A/K}^\vee}{\Lambda_{A/K}} \right)^{\text{Fr}} \right|$. If L/K is a finite extension of residue degree f and ramification degree e , then $\Lambda_{A/L} = \Lambda_{A/K}$ with (\cdot, \cdot) scaled by e , so that $\Lambda_{A/L}^\vee = \frac{1}{e} \Lambda_{A/K}^\vee$ and

$$c_{A/L} = \left| \left(\frac{\frac{1}{e} \Lambda_{A/K}^\vee}{\Lambda_{A/K}} \right)^{\text{Fr}^f} \right|.$$

Definition 3.1.3. We will refer to $d = \text{rk}_{\mathbb{Z}} \Lambda_{A/K}$ as the *toric dimension* of A/K , and to $r = \text{rk}_{\mathbb{Z}} \Lambda_{A/K}^{\text{Fr}}$ as its *split toric dimension*. Note that $d = r$ if and only if the reduction is split.

Example 3.1.4. Suppose E is an elliptic curve over K . If E has good reduction then $\Lambda = 0$, and the whole setting becomes trivial. If A has multiplicative reduction of Kodaira type I_n then $\Lambda_{A/K} = \mathbb{Z}$ and $\Lambda_{A/K}^\vee = \frac{1}{n} \mathbb{Z}$, and the pairing is $(a, b) = nab$. The Frobenius element acts either trivially on $\Lambda_{A/K}$ or as multiplication by -1 ,

corresponding to the reduction being split or non-split. The Tamagawa number can indeed be computed as

$$c_{A/K} = \left| \left(\frac{\Lambda_{A/K}^\vee}{\Lambda_{A/K}} \right)^{\text{Fr}} \right| = \left| \left(\frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}} \right)^{\text{Fr}} \right| = \begin{cases} n & \text{split multiplicative reduction,} \\ 1 & \text{non-split multiplicative reduction, } 2 \nmid n \\ 2 & \text{non-split multiplicative reduction, } 2 \mid n. \end{cases}$$

Over a finite extension L/K with ramification degree e and residue degree f , A/L has reduction type I_{en} and it has split multiplicative reduction if either A/K does or if f is even, and non-split multiplicative reduction otherwise. This is readily seen to be compatible with the above Tamagawa number formula, $c_{A/L} = |(\frac{1}{en}\mathbb{Z}/\mathbb{Z})^{\text{Fr}^f}|$.

3.2. Behaviour of Tamagawa numbers in field extensions.

Notation 3.2.1. Let K be a finite extension of \mathbb{Q}_p and A/K a semistable principally polarised abelian variety. Let Fr be the Frobenius element of K^{nr}/K . Write the characteristic polynomial of Fr acting on $\Lambda_{A/K}$ as $\pm(t-1)^r P(t)$, where $P(1) > 0$. We then define

$$\mathfrak{B}_{A/K} = \mathfrak{B}_\Lambda, \quad \mathcal{T}_{A/K} = \mathcal{T}_\Lambda, \quad P_{A/K} = P(1),$$

where $\Lambda = \Lambda_{A/K}$ with the pairing $(,)$ induced by the monodromy pairing as above.

Theorem 3.2.2. *Let K/\mathbb{Q}_p be a finite extension and A/K a semistable principally polarised abelian variety. Then $\mathcal{T}_{A/K}$ and $\mathfrak{B}_{A/K}$ are finite abelian groups and*

$$c_{A/K} = \left| \frac{\Lambda_{A/K}^{\vee \text{Fr}}}{\Lambda_{A/K}^{\text{Fr}}} \right| \cdot \frac{P_{A/K}}{|\mathcal{T}_{A/K}| |\mathfrak{B}_{A/K}|}.$$

Proof. Finiteness of \mathcal{T} and \mathfrak{B} is established in Corollary 2.3.3 and Proposition 2.2.2. The formula is a direct consequence of Theorem 2.1.1 and Proposition 2.3.2. \square

Theorem 3.2.3. *Let K/\mathbb{Q}_p be a finite extension and A/K a semistable principally polarised abelian variety. Let k be the degree of the minimal extension over which A acquires split semistable reduction, equivalently the order of the Frobenius element Fr in its action on $\Lambda_{A/K}$. For an integer m let a_m denote the multiplicity of a fixed primitive m -th root of unity among the eigenvalues of Fr acting on $\Lambda_{A/K}$, and let $b_m = 0$ or 1 according to whether $a_m = 0$ or $a_m > 0$.*

(a) $P_{A/K} = \prod_{m=q^s} q^{a_m}$ where the product is taken over all prime powers. In particular, $P_{A/K}$ remains unchanged in extensions with residue degree coprime to k .

(b) $\mathcal{T}_{A/K}$ has order dividing $P_{A/K}$ and exponent dividing $\prod_{m=q^s} q^{b_m}$, where the product is taken over all prime powers. $\mathcal{T}_{A/K}$ remains unchanged in extensions with residue degree coprime to k .

(c) $\mathfrak{B}_{A/K}$ has order dividing $P_{A/K}$ and has exponent dividing $\prod_{m=q^s} q^{b_m}$, where the product is taken over all prime powers. If L/K is an extension with residue degree coprime to k and with ramification degree e then $\mathfrak{B}_{A/L} \cong \frac{\mathfrak{B}_{A/K}}{\mathfrak{B}_{A/K}[e]}$.

$\mathfrak{B}_{A/K}$ admits a perfect antisymmetric pairing; in particular its order is either a square or twice a square. For a finite extension L/K , $\mathfrak{B}_{A/L}$ has square order if and only if at least one of the following holds: (i) $\mathfrak{B}_{A/K}$ has square order, or (ii) $[L : K]$ is even.

(d) $|\mathfrak{B}_{A/K}| \cdot |\mathcal{T}_{A/K}|$ divides $P_{A/K}$.

Proof. (a) This follows from Lemma 2.3.4.

(b) The first statement follows from Corollary 2.3.3 and the formula for $P_0(1)$ in Lemma 2.3.4. By definition, $\mathcal{T}_{A/K}$ is independent of the pairing on $\Lambda_{A/K}$, and only depends on the group generated by Fr in $\text{End}(\Lambda_{A/K})$, not on Fr itself. Hence it is unchanged in extensions with residue degree coprime to k .

(c) The first statement follows from Proposition 2.2.2 and the formula for $P_0(1)$ in Lemma 2.3.4. $\mathfrak{B}_{A/K}$ only depends on the group generated by Fr in $\text{End}(\Lambda_{A/K})$, and thus remains unchanged in unramified extensions of degree coprime to k . The general formula for $\mathfrak{B}_{A/L}$ follows from Proposition 2.1.2.

$\mathfrak{B}_{A/K}$ admits a perfect antisymmetric pairing by Proposition 2.2.2. The final claim of (c) follows from Corollary 2.4.3.

(d) This follows from Proposition 2.3.2 and the fact that, by definition, $\mathfrak{B}_{A/K}$ is a quotient of $H^1(\langle \text{Fr} \rangle, \Lambda_{A/K})$. \square

Corollary 3.2.4. *Let K/\mathbb{Q}_p be a finite extension and A/K a semistable principally polarised abelian variety of split toric dimension r . Suppose that A acquires split semistable reduction over an extension of degree k . If L/K has residue degree coprime to k and ramification degree e then*

$$c_{A/L} = |\mathfrak{B}_{A/K}[e]| \cdot c_{A/K} \cdot e^r.$$

Proof. Using Remark 3.1.2, Theorem 3.2.2 and Theorem 3.2.3 (a), (b) and the first part of (c),

$$c_{A/L} = \left| \frac{\Lambda_{A/L}^{\vee \text{Fr}}}{\Lambda_{A/L}^F} \right| \cdot \frac{P_{A/L}}{|\mathcal{T}_{A/L}| |\mathfrak{B}_{A/L}|} = \left| \frac{\frac{1}{e} \Lambda_{A/K}^{\vee \text{Fr}}}{\Lambda_{A/K}^{\text{Fr}}} \right| \cdot \frac{P_{A/K} |\mathfrak{B}_{A/K}[e]|}{|\mathcal{T}_{A/K}| |\mathfrak{B}_{A/K}|} = e^r \cdot c_{A/K} \cdot |\mathfrak{B}_{A/K}[e]|.$$

\square

Remark 3.2.5. To determine the Tamagawa number of A over every extension M/K it suffices to know $c_{A/L}$, $\mathfrak{B}_{A/L}$ and the split toric dimension of A/L just for the intermediate fields $K \subseteq L \subseteq K'$, where K'/K is the minimal unramified extension over which A acquires split semistable reduction. Indeed, one can then simply apply Corollary 3.2.4 to the extension $M/M \cap K'$ to find $c_{A/M}$.

Remark 3.2.6. Theorem 3.2.3 often lets one determine $\mathfrak{B}_{A/K}$, $\mathcal{T}_{A/K}$ and $P_{A/K}$. For instance, all three invariants are trivial if the reduction is split semistable, or if none of the eigenvalues of Fr in its action on $\Lambda_{A/K}$ have prime power order — this condition forces $P_{A/K} = 1$ by (a), and hence trivialises $\mathfrak{B}_{A/K}$ and $\mathcal{T}_{A/K}$ by (d). If instead A/K has split toric dimension 0 (i.e. Fr has no eigenvalue 1), then $\mathcal{T}_{A/K}$ is trivial by definition.

In general, $P_{A/K}$ can always be read off from the eigenvalues of Fr . Moreover one can show that the number of generators required for $\mathcal{T}_{A/K}$ and $\mathfrak{B}_{A/K}$ is at most $\min(r, d-r)$ and $(d-r)$ respectively, where d (resp. r) is the toric dimension (resp. split toric dimension) of A/K .

Lemma 2.5.2(iii) and Theorem 2.6.2 describe these invariants in special cases. The second of these translates to a classification for the case of toric dimension 2, see Theorem 3.3.2 below. The first of these gives the following result: suppose $k > 1$ and the eigenvalues of Fr are precisely the set of primitive k -th roots of unity (each occurring once), equivalently $\Lambda_{A/K} \otimes_{\mathbb{Z}} \mathbb{Q}$ is the unique faithful rational representation of $C_k = \langle \text{Fr} \rangle$. Then $\mathcal{T}_{A/K}$ is trivial; $P_{A/K} = q$ if $n = q^s$ is a prime

power, and $P_{A/K} = 1$ otherwise; $\mathfrak{B}_{A/K}$ is trivial unless $k = 2^s$ and $[\Lambda_{A/K}^\vee : \Lambda_{A/K}]$ is odd, in which case $\mathfrak{B}_{A/K} \simeq \mathbb{Z}/2\mathbb{Z}$. In particular, by Theorem 3.2.2,

$$c_{A/K} = \begin{cases} q & \text{if } k = q^s, q \text{ an odd prime,} \\ 2 & \text{if } k = 2^s \text{ and } [\Lambda_{A/K}^\vee : \Lambda_{A/K}] \text{ is even,} \\ 1 & \text{otherwise.} \end{cases}$$

Example 3.2.7. As in Example 3.1.4 consider an elliptic curve A/K with multiplicative reduction of type I_n . In this case $\mathcal{T}_{A/K}$ is trivial, and $P_{A/K}$ is 1 or 2 depending on whether the reduction is split or non-split, as one readily sees either from the definitions or from Theorem 3.2.3(a,b). By Theorem 3.2.3(c), the group $\mathfrak{B}_{A/K}$ is trivial if the reduction is split and is either trivial or $\mathbb{Z}/2\mathbb{Z}$ in the non-split case. In fact it is $\mathbb{Z}/2\mathbb{Z}$ if and only if the reduction is non-split and n is odd, as can be checked direct from the definition or using the final part of Remark 3.2.6.

Note that $\left| \frac{\Lambda_{A/K}^{\vee \text{Fr}}}{\Lambda_{A/K}^{\text{Fr}}} \right|$ is either n or 1 depending on whether the reduction is split or not, and thus the expression

$$\left| \frac{\Lambda_{A/K}^{\vee \text{Fr}}}{\Lambda_{A/K}^{\text{Fr}}} \right| \cdot \frac{P_{A/K}}{|\mathcal{T}_{A/K}| |\mathfrak{B}_{A/K}|} = \begin{cases} n & \text{for split multiplicative reduction,} \\ 1 & \text{for non-split multiplicative reduction, } 2 \nmid n \\ 2 & \text{for non-split multiplicative reduction, } 2 \mid n, \end{cases}$$

from Theorem 3.2.2 does indeed compute the local Tamagawa number in each case, cf. Example 3.1.4. This also recovers the formula in Remark 3.2.6 for the case of non-split multiplicative reduction.

Now consider a finite extension M/K with residue degree f and ramification degree e . If A/K has split multiplicative reduction, then

$$c_{A/M} = en = c_{A/K} \cdot e,$$

as predicted by Corollary 3.2.4 with $r = 1$ and trivial $\mathfrak{B}_{A/K}$. If A/K has non-split multiplicative reduction, then it becomes split over the quadratic unramified extension K'/K . One readily checks that

$$c_{A/M} = \begin{cases} |\mathfrak{B}_{A/K}[e]| \cdot c_{A/K} & \text{if } 2 \nmid f, \\ c_{A/K'} \cdot e & \text{if } 2 \mid f, \end{cases}$$

again as predicted by Corollary 3.2.4, with $r = 0, 1$ over K and K' , respectively, and trivial $\mathfrak{B}_{A/K'}$. This illustrates Remark 3.2.5, that to obtain $c_{A/M}$ over general extensions one just needs to know $c_{A/L}$, $\mathfrak{B}_{A/L}$ and r for the subfields $K \subseteq L \subseteq K'$, where K' is the minimal extension over which the reduction becomes split semistable. Thus in general, the cases “ $2 \mid f$ ” and “ $2 \nmid f$ ” will be replaced by the possible values of $\gcd(f, k)$, where $k = [K' : K]$.

Corollary 3.2.8. *Let K/\mathbb{Q}_p be a finite extension and A/K a semistable abelian variety. If $K \subset L_1 \subset L_2 \subset \dots$ is a tower of finite field extensions with L_t/K of ramification degree e_t , then for all sufficiently large t*

$$c_{A/L_t} = C \cdot e_t^{r_\infty},$$

for some suitable constant $C \in \mathbb{Q}$, and where r_∞ is the split toric dimension of A/L_t for all sufficiently large t .

Proof. We begin by reducing to the case of principally polarised abelian varieties. Note first that A/L and the dual abelian variety A^*/L have the same Tamagawa number and the same split toric dimension over any extension L/K . Indeed, let Φ and Φ' denote the Néron component groups of A/L and of A^*/L , respectively. They admit a perfect $\text{Gal}(L^{nr}/L)$ -invariant pairing $\Phi \times \Phi' \rightarrow \mathbb{Q}/\mathbb{Z}$ ([7] §11.4) and

$$c_{A/L} = \Phi^{\text{Gal}(L^{nr}/L)} \quad \text{and} \quad c_{A^*/L} = \Phi'^{\text{Gal}(L^{nr}/L)},$$

so, in particular, $c_{A/L} = c_{A^*/L}$. They have the same split toric dimension since they are isogenous (polarisation) and, in particular, have isogenous l -adic Tate modules. It thus suffices to prove the theorem for the abelian variety $A^4 \times A^{*4}$, which, by Zarhin's trick, admits a principal polarisation. In other words, we may assume that A/K is principally polarised.

We may replace K by the maximal unramified extension of K in $\bigcup L_t$ whose degree divides k , the order of the Frobenius element Fr in its action on $\Lambda_{A/K}$. Indeed, this extension is also contained in L_t for all sufficiently large t , and this operation alters neither the e_t nor r_∞ . This now ensures that the residue degrees of L_t/K are all coprime to k , and also gives $r = r_\infty$. The result now follows from Corollary 3.2.4, since the sequence $\mathfrak{B}_{A/K}[e_t]$ is eventually constant. \square

Remark 3.2.9. The analogue of Corollary 3.2.8 can fail for non-semistable reduction. For example, the Tamagawa number of the elliptic curve 243a1 fluctuates between 1 and 3 in the layers of the cyclotomic \mathbb{Z}_3 -tower of \mathbb{Q}_3 , see [5] Remark 5.4.

Theorem 3.2.10. *Let K be a finite extension of \mathbb{Q}_p , and let A/K be a semistable principally polarised abelian variety of toric dimension d and split toric dimension r . If L/K is a finite extension with residue degree f and ramification degree e , then*

$$c_{A/L} \sim \begin{cases} c_{A/K} \cdot e^r & \text{if } 2 \nmid e, 2 \nmid f, \\ c_{A/K} \cdot |\mathfrak{B}_{A/K}| \cdot e^r & \text{if } 2 \mid e, 2 \nmid f, \\ c_{A/K^{nr}} \cdot e^d & \text{if } 2 \mid f, \end{cases}$$

where \sim denotes equality up to rational squares.

Proof. This follows from Theorem 2.4.2, noting that $c_{A/K^{nr}} = \left| \frac{\Lambda_{A/K}^\vee}{\Lambda_{A/K}} \right|$. \square

Remark 3.2.11. Recall that the group $\mathfrak{B}_{A/K}$ admits a perfect antisymmetric pairing, and so it has square order if and only if it admits a perfect alternating pairing. Thus Theorems 3.2.3(c) and 3.2.10 may be reformulated in this language. (Note, however, that this is not equivalent to *every* perfect antisymmetric pairing on $\mathfrak{B}_{A/K}$ being alternating.)

3.3. Classification for dimension 2.

Definition 3.3.1. Let K be a finite extension of \mathbb{Q}_p and A/K a semistable principally polarised abelian variety of toric dimension 2. Recall that $\Lambda_{A/K} \subseteq \Lambda_{A/K}^\vee$ are Fr -invariant 2-dimensional lattices, dual to each other with respect to a symmetric \mathbb{Q} -valued pairing. Such lattices are classified in Theorem 2.6.2. We will say that A/K has a certain *reduction type* if $\Lambda_{A/K}, \Lambda_{A/K}^\vee$ have this type in that classification.

Thus the possible reduction types are $[1.1 : n, m]$, $[1.2_A : n, m]$, $[1.2_B : n, m]$, $[2.2 : n, m]$, $[3 : n]$, $[4 : n]$ and $[6 : n]$, where the parameters n and m are positive integers with $n \equiv m \pmod{2}$ for type $[1.2_B : n, m]$. Types $[1.1 : n_1, m_1]$ and

$[1.1 : n_2, m_2]$ are the same if and only if $C_{n_1} \times C_{m_1} \simeq C_{n_2} \times C_{m_2}$, and similarly for types $[2.2 : -]$. All other types are distinct. Recall that the first digits of the type name specify the orders of the eigenvalues of the Frobenius element acting on $\Lambda_{A/K}$. In particular, A/K acquires split semistable reduction over an unramified extension of degree 1, 2, 2, 2, 3, 4 and 6 for the seven types, respectively.

Theorem 3.3.2. *Let K/\mathbb{Q}_p be a finite extension and let A/K be a semistable principally polarised abelian variety of toric dimension 2. Then its Tamagawa number depends on its type as listed in the following table:*

Type	$c_{A/K}$	$f = 2$	$f = 3$
$[1.1 : n, m]$	nm	<i>unchanged</i>	<i>unchanged</i>
$[1.2_A : n, m]$	n (m odd) $2n$ (m even)	$[1.1 : n, m]$	<i>unchanged</i>
$[1.2_B : n, m]$	n	$[1.1 : 2n, m/2]$ ($\text{ord}_2 \frac{n}{m} > 0$) $[1.1 : n, m]$ ($\text{ord}_2 \frac{n}{m} = 0$) $[1.1 : n/2, 2m]$ ($\text{ord}_2 \frac{n}{m} < 0$)	<i>unchanged</i>
$[2.2 : n, m]$	1 (n, m odd) 2 (n, m odd/even) 4 (n, m even)	$[1.1 : n, m]$	<i>unchanged</i>
$[3 : n]$	3	<i>unchanged</i>	$[1.1 : n, 3n]$
$[4 : n]$	1 (n odd) 2 (n even)	$[2.2 : n, n]$	<i>unchanged</i>
$[6 : n]$	1	$[3 : n]$	$[2.2 : n, 3n]$

Taking the base change of A/K to a totally ramified extension of degree e does not change its reduction type, but scales the parameters n and m by e . An unramified extension of degree coprime to 2 and 3 does not change the type or the parameters. An unramified extension of degree 2 or 3 changes the type as shown in the table, corresponding to the columns “ $f = 2$ ” and “ $f = 3$ ”.

Proof. By Remark 3.1.2, the Tamagawa number is given by $c_{A/K} = \left| \left(\frac{\Lambda_{A/K}^\vee}{\Lambda_{A/K}} \right)^{\text{Fr}} \right|$.

The classification of the Tamagawa numbers then follows from Theorem 2.6.2 with $\Lambda = \Lambda_{A/K}$. By the same Remark, a totally ramified extension changes $\Lambda_{A/K}^\vee$ to $\frac{1}{e}\Lambda_{A/K}^\vee$, which in turn scales the parameters of the type by e (see Remark 2.6.3(iv)).

An unramified extension does not change $\Lambda_{A/K}$ or $\Lambda_{A/K}^\vee$, but changes Fr to Fr^f . Thus the claim for unramified extensions follows from Theorem 2.6.2, by a case-by-case analysis: all cases are straightforward, except perhaps that of cubic extensions for types $[3 : -]$ and $[6 : -]$, and quadratic extensions for $[1.2_B : -]$.

To see the effect of a cubic unramified extension for the type $[3 : n]$ (respectively $[6 : n]$), note that $\mathbb{Z}[\zeta_3]/(\zeta_3 - 1)n\mathbb{Z}[\zeta_3] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$ as abelian groups, so it becomes $[1.1 : n, 3n]$ (respectively, $[2.2 : n, 3n]$), as claimed.

Similarly, for a quadratic unramified extension for type $[1.2_B : n, m]$, note that $\frac{\mathbb{Z} \oplus \mathbb{Z} + \langle \frac{1}{2}, \frac{1}{2} \rangle}{n\mathbb{Z} \oplus m\mathbb{Z} + \langle \frac{n}{2}, \frac{m}{2} \rangle} \simeq C_{2n} \times C_{m/2}$ or $C_n \times C_m$ or $C_{n/2} \times C_{2m}$, depending on whether $\text{ord}_2 n > \text{ord}_2 m$, $\text{ord}_2 n = \text{ord}_2 m$ or $\text{ord}_2 n < \text{ord}_2 m$, respectively — this gives the claimed description. (To see this isomorphism of abelian groups, write $n = n'2^a$,

$m = m'2^b$ with odd n', m' . The quotient group is closely related to the elementary group $\frac{\mathbb{Z} \oplus \mathbb{Z}}{n\mathbb{Z} \oplus m\mathbb{Z}}$ by the exact sequence $C_2 \rightarrow \frac{\mathbb{Z} \oplus \mathbb{Z}}{n\mathbb{Z} \oplus m\mathbb{Z}} \rightarrow \frac{\mathbb{Z} \oplus \mathbb{Z} + \langle \frac{1}{2}, \frac{1}{2} \rangle}{n\mathbb{Z} \oplus m\mathbb{Z} + \langle \frac{n}{2}, \frac{m}{2} \rangle} \rightarrow C_2$, and so it is isomorphic to one of $C_n \times C_m$, $C_{2n} \times C_{m/2}$ or $C_{n/2} \times C_{2m}$. If $a = b$, then $(1, 0)$, $(0, 1)$ and $(\frac{1}{2}, \frac{1}{2})$ are all killed by $2^a n' m' = nm' = n'm$ in the quotient group. Thus there are no elements of order 2^{a+1} , and hence the group is $C_n \times C_m$. If instead, without loss of generality, $a > b$, then $2^a n' m' (\frac{1}{2}, \frac{1}{2}) = (\frac{nm'}{2}, \frac{2^{a-b} n'm}{2}) \equiv (\frac{n}{2}, 0)$ in the quotient group. So $(\frac{n'm'}{2}, \frac{n'm'}{2})$ has order 2^{a+1} and the group must be $C_{2n} \times C_{m/2}$. \square

3.4. Applications to the p -parity conjecture. We finally turn to abelian varieties over number fields. Recall from §1.3 that for an abelian variety A over a number field K we write $\mathcal{X}_p(A/K)$ for its dual p^∞ -Selmer group. This is a \mathbb{Q}_p -vector space whose dimension is, conjecturally, the rank of A/K . The p -parity conjecture (Conjecture 1.3.1) states that the parity of this dimension can be read off from the global root number $w(A/K)$. More generally, if F/K is a finite Galois extension and τ a self-dual complex representation of $\text{Gal}(F/K)$, then it gives a formula for the parity of the multiplicity of τ in $\mathcal{X}_p(A/F)$:

$$(-1)^{\langle \mathcal{X}_p(A/F), \tau \rangle} = w(A/K, \tau),$$

where $w(A/K, \tau)$ is the root number of the twist of A/K by τ , and $\langle \cdot, \cdot \rangle$ the usual inner product of characters of a finite group. (Strictly speaking, we first need to fix an embedding $\mathbb{Q}_p \subset \mathbb{C}$, so as to be able to compare complex and p -adic representations. We do this once and for all.)

The aim of this section is to prove the p -parity conjecture for a specific supply $\mathbf{T}_p^{F/K}$ of twisting representations τ (Theorem 3.4.10). The approach relies on the theory of Brauer relations and regulator constants of [3].

Notation 3.4.1. Let G be a finite group. We say that a formal \mathbb{Z} -linear combination of (conjugacy classes of) subgroups $\Theta = \sum_i n_i H_i$ is a Brauer relation (or a G -relation), if

$$\bigoplus_i \mathbb{C}[G/H_i]^{\oplus n_i} \simeq 0$$

as a virtual representation, i.e. if the character $\sum_i n_i \chi_{\mathbb{C}[G/H_i]} = 0$.

Fix a prime p . For a self-dual \mathbb{Q}_p -representation ρ of G we then define its regulator constant as

$$\mathcal{C}_\Theta(\rho) = \prod_i \det \left(\frac{1}{|H_i|} (\cdot, \cdot) \mid \rho^{H_i} \right) \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2},$$

where (\cdot, \cdot) is any non-degenerate G -invariant pairing on ρ , and the determinant is computed on any \mathbb{Q}_p -basis of the invariant subspace ρ^{H_i} . This definition is known to be independent of the choices of the pairing and of the bases.

We now define $\mathbf{T}_{\Theta, p}$ to be the set of self-dual $\mathbb{Q}_p G$ -representations τ that satisfy

$$\langle \tau, \rho \rangle \equiv \text{ord}_p \mathcal{C}_\Theta(\rho) \pmod{2}$$

for every self-dual $\mathbb{Q}_p G$ representation ρ .

For a Galois extension F/K of number fields with Galois group G we then define

$$\mathbf{T}_p^{F/K} = \bigcup_{\Theta} \mathbf{T}_{\Theta, p},$$

where the union is taken over all the Brauer relations of G .

Remark 3.4.2. The set $\mathbf{T}_p^{F/K}$ still remains rather mysterious. In the context of the parity conjecture and Brauer relations it should be thought of as the set of “computable representations”. If, as above, F/K is a Galois extension with Galois group G and A/K an abelian variety, then $\mathcal{X}_p(A/F)$ can be decomposed into irreducible \mathbb{Q}_p -representations $\mathcal{X}_p(A/F) \simeq \bigoplus_i \rho_i^{\oplus n_i}$. Ideally, we would like to be able to determine the multiplicities n_i , but this appears to be beyond reach at present. However, the machine of Brauer relations and regulator constants gives a formula for $\sum_{i \in I} n_i \pmod 2$ for suitable sets I of representations of G . These sets I are determined by regulator constants: if Θ is a G -relation then the \mathbb{Q}_p -representations ρ for which $\text{ord}_p \mathcal{C}_\Theta(\rho)$ is odd form such a set. Now pick one \mathbb{Q}_p -irreducible constituent τ_i of each of the ρ_i for $i \in I$ and set $\tau = \bigoplus \tau_i$. The sum of the multiplicities $\sum n_i \pmod 2$ that we can compute is the same as $\langle \tau, \mathcal{X}_p(A/F) \rangle \pmod 2$. All the possible τ that can be obtained in this fashion are exactly the set $\mathbf{T}_p^{F/K}$. (Technically, to get all of $\mathbf{T}_p^{F/K}$, we also need to allow to take an odd number of constituents of ρ_i , and an even number of constituents for those self-dual ρ for which $\text{ord}_p \mathcal{C}(\rho)$ is even.)

Example 3.4.3. The group $G = S_3$ has three complex irreducible representations ($\mathbf{1}$, $\text{sign } \epsilon$ and 2-dimensional ρ) and four subgroups up to conjugacy ($S_3, C_3, C_2, \{\text{id}\}$). The corresponding permutation representations decompose as

$$\mathbb{C}[G/S_3] \simeq \mathbf{1} \quad \mathbb{C}[G/C_3] \simeq \mathbf{1} \oplus \epsilon \quad \mathbb{C}[G/C_2] \simeq \mathbf{1} \oplus \rho \quad \mathbb{C}[G/\{\text{id}\}] \simeq \mathbf{1} \oplus \epsilon \oplus \rho^{\oplus 2}.$$

Thus one easily sees that, up to multiples, S_3 has exactly one Brauer relation:

$$\Theta = 2S_3 - C_3 - 2C_2 + \{\text{id}\}.$$

Now fix any prime p . The irreducible \mathbb{Q}_p -representations of S_3 are still $\mathbf{1}, \epsilon$ and ρ , since they can all be realised over \mathbb{Q} . To compute their regulator constants we need to pick an S_3 -invariant pairing on the representations. For example, for $\mathbf{1}$ we can take the pairing $(1, 1) = 1$, or indeed any other one. We then compute

$$\mathcal{C}_\Theta(\mathbf{1}) = \left(\frac{1}{6} \cdot 1\right)^2 \left(\frac{1}{3} \cdot 1\right)^{-1} \left(\frac{1}{2} \cdot 1\right)^{-2} \left(\frac{1}{1} \cdot 1\right) = 3 \cdot \square,$$

where “ \square ” denotes a rational square. Note that choosing a different pairing would not have affected the result (the powers neatly cancel!) and that picking different bases for the invariant spaces $\mathbf{1}^H$ for the various subgroups H would only have changed the result by a square in \mathbb{Q}_p . One similarly computes the regulator constant for the other two irreducibles, which in this example give the same result: $\mathcal{C}_\Theta(\epsilon) = \mathcal{C}_\Theta(\rho) = 3$.

Now let $p = 3$. The parity of the power of 3 in the regulator constant of a representation X can simply be computed by counting the number of $\mathbf{1}, \epsilon$ and ρ in its decomposition into irreducibles (regulator constants are multiplicative). Equivalently, $\text{ord}_3 \mathcal{C}_\Theta(X) \equiv \langle \mathbf{1} \oplus \epsilon \oplus \rho, X \rangle \pmod 2$. This precisely means that $\tau = \mathbf{1} \oplus \epsilon \oplus \rho \in \mathbf{T}_{\Theta, 3}$.

The purpose of this machine is that we can prove the 3-parity conjecture for twists by representations like τ : Theorem 3.4.10 shows that if F/K is an extension of number fields with Galois group S_3 , then the 3-parity conjecture holds for a large class of abelian varieties over K twisted by the representation τ of $\text{Gal}(F/K)$.

Notation 3.4.4. For an abelian variety over a local field A/K together with a non-zero regular exterior form ω , we write

$$C(A/K, \omega) = \begin{cases} c_{A/K} \cdot \left| \frac{\omega}{\omega^\circ} \right|_K & \text{for } K \text{ non-archimedean,} \\ \int_{A(K)} |\omega| & \text{for } K = \mathbb{R}, \\ 2^{\dim A} \int_{A(K)} |\omega \wedge \bar{\omega}| & \text{for } K = \mathbb{C}, \end{cases}$$

where $|\cdot|_K$ is the normalised absolute value of K and ω° is the Néron exterior form. If F/K is a Galois extension and $\Theta = \sum_i n_i H_i$ a Brauer relation in its Galois group, we use the shorthand notation

$$C_v(\Theta) = \prod_i C(A/F^{H_i}, \omega)^{n_i}.$$

This quantity is independent of the choice of ω (see [3] Notation 3.1). The subscript “ v ” is there only to indicate that the setting is local.

If K is instead a number field, we write $C_{A/K} = \prod_v C(A/K_v, \omega)$, the product taken over all the places of K . This definition is independent of the choice of ω by the product formula. We similarly write

$$C(\Theta) = \prod_i C(A/F^{H_i})^{n_i},$$

whenever F/K is a Galois extension and $\Theta = \sum_i n_i H_i$ a Brauer relation in its Galois group.

Definition 3.4.5. Let K be a local field, A/K an abelian variety and p a fixed prime number. For a Galois extension F/K , let us say that *local compatibility holds for A in F/K* if for every Brauer relation Θ of $\text{Gal}(F/K)$ and every $\tau \in \mathbf{T}_{\Theta, p}$,

$$(-1)^{\text{ord}_p C_v(\Theta)} = w(A/K, \tau).$$

We will also say that *local compatibility holds for A/K* if it holds for A in all Galois extensions F/K .

Theorem 3.4.6. *Let F/K be a Galois extension of number fields, p a prime number, and A/K an abelian variety. Suppose that local compatibility holds for A in F_w/K_v at every place v of K and every place $w|v$ of F . Then*

$$(-1)^{\text{ord}_p C(\Theta)} = w(A/K, \tau)$$

for every $\text{Gal}(F/K)$ -relation Θ and every $\tau \in \mathbf{T}_{\Theta, p}$.

Suppose further that A is principally polarised. Then the p -parity conjecture holds for all twists of A/K by $\tau \in \mathbf{T}_p^{F/K}$.

Proof. This is essentially proved in the beginning of §3 of [3], although unfortunately not stated there in this form. We will not repeat the proof here, as it requires quite a lot of notation and several general results from [3]. We will just explain which parts need to be taken and how they need to be modified.

The first part of the theorem follows from the proof of [3] Cor. 3.4.: the single use in that proof of [3] Thm. 3.2. (in the form of Cor. 3.3.) is replaced by our hypothesis that local compatibility holds for A in F_w/K_v at all v . The rest of the proof of [3] Cor. 3.4. holds verbatim.

The second part of the theorem follows from the proof of [3] Thm. 1.6., (after the proof of Cor. 3.4). It is a simple application of [3] Thm. 1.14. Strictly speaking, [3] Thm. 1.14 imposes the extra hypothesis that if $p = 2$ then the principal

polarisation on A/K is induced by a K -rational divisor. This assumption ensures that $\text{III}^\circ(A/L)[p^\infty]$ has square order for every prime p and every finite extension L/K , and is used in the proof solely to guarantee that

$$\prod_i |\text{III}^\circ(A/F^{H_i})[p^\infty]|^{n_i} \in \mathbb{Q}^{\times 2},$$

for every Brauer relation $\sum n_i H_i$ of $\text{Gal}(F/K)$. (Here III° denotes the Tate–Shafarevich group modulo its divisible part.) In fact, the “non-squaredness of III ” always cancels in Brauer relations as shown in the theorem below, so this extra hypothesis is unnecessary. \square

Theorem 3.4.7 (see also [10] Cor. A.1). *Let F/K be a Galois extension and A/K a principally polarised abelian variety. Then for every Brauer relation $\Theta = \sum_i n_i H_i$ of $\text{Gal}(F/K)$ and every prime p ,*

$$\prod_i |\text{III}^\circ(A/F^{H_i})[p^\infty]|^{n_i} \in \mathbb{Q}^{\times 2},$$

where III° denotes the Tate–Shafarevich group modulo its divisible part.

Proof. When p is odd (or the polarisation is induced by a K -rational divisor), this is true because each term $\text{III}^\circ(A/F^{H_i})[p^\infty]$ has square order. For $p = 2$ this is slightly more delicate. As was observed independently by Cesnavicius and Poonen, and by Morgan (see [10] Prop. A.1), the non-square part of III behaves well in field extensions: if L/K is a finite extension then

$$|\text{III}^\circ(A/L)[2^\infty]| = |\text{III}^\circ(A/K)[2^\infty]|^{[L:K]} \cdot \square,$$

where “ \square ” denotes a rational square. Hence

$$\begin{aligned} \prod_i |\text{III}^\circ(A/F^{H_i})[2^\infty]|^{n_i} &= \prod_i |\text{III}^\circ(A/K)[2^\infty]|^{n_i \dim \mathbb{C}[G/H_i]} \cdot \square = \\ &= |\text{III}^\circ(A/K)[2^\infty]|^{\sum_i n_i \dim \mathbb{C}[G/H_i]} \cdot \square = \square. \end{aligned}$$

\square

Lemma 3.4.8. *Local compatibility holds for all abelian varieties in cyclic extensions of local fields.*

Proof. Cyclic groups have no Brauer relations, so there is nothing to prove. \square

Theorem 3.4.9. *Local compatibility holds for all semistable principally polarised abelian varieties over local fields of characteristic zero.*

Proof. For archimedean local fields this follows from the previous lemma.

Suppose F/K is a finite Galois extension of l -adic fields. Let p be a prime number, A/K a semistable principally polarised abelian variety, $\Theta = \sum n_i H_i$ a $\text{Gal}(F/K)$ -relation and $\tau \in \mathbf{T}_{\Theta,p}$. Write d and r for the toric dimension and the split toric dimension of A/K , respectively, and $\Lambda = \Lambda_{A/K} \otimes_{\mathbb{Z}} \mathbb{Q}_p$.

The root number of the twist is given by

$$w(A/K, \tau) = w(\tau)^{2 \dim A} (-1)^{\langle \tau, \Lambda \rangle} = (-1)^{\langle \tau, \Lambda \rangle},$$

where the first equality is a standard formula for the root number of a twist of a semistable abelian variety by a self-dual representation, and the second follows from the determinant formula $w(\sigma)w(\sigma^*) = \det \sigma(-1)$ and the fact that all elements of $\mathbf{T}_{\Theta,p}$ have trivial determinant, see [3] Prop. 3.23., Lemma A.1 and Thm. 2.56.

Let ω be a minimal exterior form on A/K . As A/K is semistable, ω remains minimal over every extension L/K , so that

$$C(A/L, \omega) = c_{A/L} = \begin{cases} c_{A/K} \cdot e^r \cdot \square & \text{if } 2 \nmid e, 2 \nmid f, \\ c_{A/K} \cdot |\mathfrak{B}_{A/K}| \cdot e^r \cdot \square & \text{if } 2 \mid e, 2 \nmid f, \\ c_{A/K^{nr}} \cdot e^d \cdot \square & \text{if } 2 \mid f, \end{cases}$$

by Theorem 3.2.10, where e and f denote the ramification and the residue degree of L/K , respectively.

We now proceed to show that $(-1)^{\text{ord}_p C_v(\Theta)} = w(A/K, \tau)$ by using these explicit formulas for both terms. Rather than doing the computation for the behaviour of these functions in Brauer relations from scratch, we will take a shortcut by making use of the fact that the theorem has already been established for semistable elliptic curves in [3] Prop. 3.9. If E_1, E_2 and E_3 are elliptic curves with, respectively, split multiplicative reduction of type I_1 and non-split multiplicative reduction of types I_1 and I_2 , then their Tamagawa numbers over L are

$$c_1(L) = c_{E_1/L} = e, \quad c_2(L) = c_{E_2/L} = \begin{cases} 1, & \text{if } 2 \nmid e, 2 \nmid f \\ 2, & \text{if } 2 \mid e, 2 \nmid f \\ e, & \text{if } 2 \mid f \end{cases}, \quad c_3(L) = c_{E_3/L} = \begin{cases} 2, & \text{if } 2 \nmid f \\ 2e, & \text{if } 2 \mid f \end{cases}.$$

Thus we already know that

$$\text{ord}_p c_1(\Theta) \equiv \langle \tau, \mathbf{1} \rangle, \quad \text{ord}_p c_2(\Theta) \equiv \langle \tau, \chi \rangle, \quad \text{ord}_p c_3(\Theta) \equiv \langle \tau, \chi \rangle,$$

where $c_j(\Theta) = \prod_i c_j(F^{H_i})^{n_i}$, χ denotes the unramified character of order 2 of K , and \equiv is equality mod 2.

Since the Galois group acts on Λ through a finite cyclic quotient, and this representation is unramified and self-dual,

$$\Lambda \simeq \mathbf{1}^{\oplus r} \oplus \chi^{\oplus s} \oplus (\rho \oplus \rho^*)$$

for some representation ρ and some integer $s \equiv d - r \pmod{2}$.

Note that we can factor

$$C(A/L, \omega) = \gamma \left(\frac{2c_2}{c_3} \right)^\eta c_1^r \left(\frac{c_3}{2} \right)^{d-r} \cdot \square,$$

where $\gamma = \gamma(L) = \begin{cases} c_{A/K}, & \text{if } 2 \nmid f \\ c_{A/K^{nr}}, & \text{if } 2 \mid f \end{cases}$ and η is 0 or 1 depending on whether $|\mathfrak{B}_{A/K}|$ is a square or twice a square (Theorem 3.2.3(c)). Set $\gamma'(L) = 2^{\eta-d+r} \gamma(L)$ and write $\gamma'(\Theta) = \prod_i \gamma'(F^{H_i})^{n_i}$. Then

$$C_v(\Theta) = \gamma'(\Theta) \left(\frac{c_2(\Theta)}{c_3(\Theta)} \right)^\eta c_1(\Theta)^r c_3(\Theta)^{d-r} \cdot \square.$$

As a function of the field L , γ' depends only on the residue degree f , and hence $\gamma'(\Theta) = 1$; this is a general fact about evaluating such functions on Brauer relations, see [3] Thm. 2.36(f). Hence

$$\text{ord}_p C_v(\Theta) \equiv r \langle \tau, \mathbf{1} \rangle + (d - r) \langle \tau, \chi \rangle \equiv \langle \tau, \mathbf{1}^{\oplus r} \oplus \chi^{\oplus s} \rangle \equiv \langle \tau, \Lambda \rangle \pmod{2},$$

because $s \equiv d - r \pmod{2}$ and τ is self-dual. By the formula for the root number above,

$$(-1)^{\text{ord}_p C_v(\Theta)} = w(A/K, \tau),$$

as required. \square

Theorem 3.4.10. *Let F/K be a Galois extension of number fields and let p be a prime number. Let A/K be a principally polarised abelian variety all of whose primes of non-semistable reduction have cyclic decomposition groups in F/K . Then the p -parity conjecture holds for all twists of A/K by $\tau \in \mathbf{T}_p^{F/K}$.*

Proof. This follows from Lemma 3.4.8, Theorem 3.4.9 and Theorem 3.4.6. \square

4. APPENDIX: INTEGRAL MODULE STRUCTURE OF $\Lambda_{A/K}$ FOR JACOBIANS OF SEMISTABLE HYPERELLIPTIC CURVES OF GENUS 2

by Vladimir Dokchitser and Adam Morgan

In this appendix we explain how the “lattice type”, in the sense of Theorem 1.2.2, of the character group $\Lambda_{J/K}$ of the toric part of the reduction can be determined when J is the Jacobian of a semistable hyperelliptic curve of genus 2. Theorem 1.2.2 then lets one read off the Tamagawa number of J over all finite extensions of the base field.

Let p be an odd prime and K/\mathbb{Q}_p a finite extension. Let \mathcal{C}/K be a hyperelliptic curve given by an equation

$$\mathcal{C}: y^2 = f(x),$$

with $f(x) \in \mathcal{O}_K[x]$ with no repeated roots in \overline{K} . Write $J = \text{Jac}(\mathcal{C})$ for the Jacobian of \mathcal{C} . The article [6] provides an explicit criterion that determines whether \mathcal{C} is semistable, and, under this assumption, a description of its minimal regular model and its special fibre (together with the Frobenius action) and of the lattice $\Lambda_{A/K}$. Here we apply this machinery in the case when \mathcal{C} has genus 2 to obtain the lattice type of $\Lambda_{J/K}$ in terms of elementary data attached to $f(x)$. We omit the proofs and computations, which will be included in [6].

The description is similar to the familiar one for elliptic curves with multiplicative reduction, corresponding to the case when $f(x)$ is a cubic whose reduction has a double root in $\overline{\mathbb{F}}_p$. There one checks the tangents at the singular point to decide whether the reduction is split or non-split multiplicative, and the valuation of the discriminant (equivalently, twice the valuation of the difference of the two roots that have the same reduction) to determine the parameter n of the Kodaira type I_n .

For the purposes of this appendix we assume that $f(x)$ has degree 5 or 6, so that \mathcal{C} has genus 2, and impose the following simplifying assumption:

- $f(x)$ has a unit leading coefficient and its reduction $\bar{f}(x)$ has no triple roots in $\overline{\mathbb{F}}_p$. (In particular, \mathcal{C} and J have semistable reduction.)

For a double root $\alpha \in \overline{\mathbb{F}}_p$ of $\bar{f}(x)$ define the two “tangents” t_α^\pm by

$$t_\alpha^\pm = \pm \sqrt{g(\alpha)}, \quad \text{where} \quad \bar{f}(x) = (x - \alpha)^2 g(x),$$

and define the pairs

$$A^\pm = (\alpha, t_\alpha^\pm).$$

Also set

$$a = 2 \cdot v_K(\alpha_1 - \alpha_2) \in \mathbb{Z},$$

where $\alpha_1, \alpha_2 \in \overline{K}$ are the two roots of $f(x)$ that reduce to α , and the valuation $v_K : \overline{K}^\times \rightarrow \mathbb{Q}$ is normalised so as to send the uniformiser of \mathcal{O}_K to 1. If there are

further double roots of $\bar{f}(x)$ present, say β and γ , we similarly define the quantities $t_\beta^\pm, t_\gamma^\pm, B^\pm, C^\pm$ and b, c , corresponding to these roots.

The type of the lattice $\Lambda_{J/K}$ can be read off from the valuations a, b, c and the action of the Frobenius automorphism on A^\pm, B^\pm, C^\pm as shown in the following table. For convenience of the reader, the table also lists the order of Frobenius in this action, the Tamagawa number $c_{J/K}$ and the toric dimension of J , equivalently the rank of $\Lambda_{J/K}$. The lattices and their properties are described in Theorem 1.2.2, Lemma 2.6.1 and Theorem 2.6.2. We use the shorthand notation

$$\tilde{x} = 1 \text{ if } x \text{ is odd,} \quad \tilde{x} = 2 \text{ if } x \text{ is even,}$$

and

$$d = \gcd(a, b, c), \quad n = ab + bc + ac,$$

in the case when \bar{f} has three double roots.

Double roots of \bar{f}	Order of Frobenius	Orbits of Frobenius on pairs	Toric dimension	Lattice type of $\Lambda_{J/K}$	Tamagawa number
none	—	—	0	—	1
α	1	$\{A^+\} \quad \{A^-\}$	1	$[1:a]$	a
α	2	$\{A^+, A^-\}$	1	$[2:a]$	\tilde{a}
α, β	1	$\{A^+\} \quad \{A^-\} \quad \{B^+\} \quad \{B^-\}$	2	$[1.1 : a, b]$	$a \cdot b$
α, β	2	$\{A^+, A^-\} \quad \{B^+\} \quad \{B^-\}$	2	$[1.2_A : a, b]$	$a \cdot \tilde{b}$
α, β	2	$\{A^+, A^-\} \quad \{B^+, B^-\}$	2	$[2.2 : a, b]$	$\tilde{a} \cdot \tilde{b}$
α, β	2	$\{A^+, B^+\} \quad \{A^-, B^-\}$	2	$[1.2_B : a, a]$	a
α, β	4	$\{A^+, B^+, A^-, B^-\}$	2	$[4 : a]$	\tilde{a}
α, β, γ	1	$\{A^+\} \quad \{A^-\} \quad \{B^+\} \quad \{B^-\} \quad \{C^+\} \quad \{C^-\}$	2	$[1.1 : d, n/d]$	\widetilde{n}
α, β, γ	2	$\{A^+, A^-\} \quad \{B^+, B^-\} \quad \{C^+, C^-\}$	2	$[2.2 : d, n/d]$	$\tilde{d} \cdot \widetilde{n/d}$
α, β, γ	2	$\{A^+, B^+\} \quad \{A^-, B^-\} \quad \{C^+\} \quad \{C^-\}$	2	$[1.2_B : a+2c, a]$	$a+2c$
α, β, γ	2	$\{A^+, B^+\} \quad \{A^-, B^-\} \quad \{C^+, C^-\}$	2	$[1.2_B : a, a+2c]$	a
α, β, γ	3	$\{A^+, B^+, C^+\} \quad \{A^-, B^-, C^-\}$	2	$[3 : a]$	3
α, β, γ	6	$\{A^+, B^+, C^+, A^-, B^-, C^-\}$	2	$[6 : a]$	1

Let us remark that the table is complete, in the sense that these are all the possible Frobenius actions on the pairs under our hypotheses on $f(x)$. It is also not too difficult to check that by varying $f(x)$ it is possible to obtain all the lattice types of Theorem 1.2.2 with all possible parameter values.

Example 4.1.1. Let \mathcal{C}/\mathbb{Q}_3 be given by the equation

$$y^2 = f(x)$$

with

$$f(x) = x^5 + x^4 + 20x^3 + 20x^2 + 64x + 64.$$

Over the residue field, this polynomial factorises as $\bar{f}(x) = (x+i)^2(x-i)^2(x+1)$, where $i \in \mathbb{F}_9$ denotes a square root of -1 . It visibly has the double roots $\alpha = i$ and $\beta = -i$, along with the single root -1 . Moreover

$$t_\alpha^\pm = \pm\sqrt{(\alpha+i)^2(\alpha+1)} = \pm iw, \quad t_\beta^\pm = \pm\sqrt{(\beta-i)^2(\beta+1)} = \pm iw^3,$$

where w denotes a square root of $1+i$ in \mathbb{F}_{81} (a 16th root of unity). Thus the pairs we need to determine the reduction type are $A^\pm = (i, \pm iw)$ and $B^\pm = (-i, \pm iw^3)$.

Frobenius acts on these as the 4-cycle $(A^+B^-A^-B^+)$, so the table gives the associated lattice type as $[4 : a]$ for some $a \in \mathbb{Z}$.

Over $\overline{\mathbb{Q}}_3$, the polynomial factors as $f(x) = ((x-i)^2+9)((x+i)^2+9)(x+1)$, where i now denotes a square root of -1 in $\overline{\mathbb{Q}}_3$. Writing α_1, α_2 for the roots that reduce to α , we find that

$$a = 2 \cdot v_{\mathbb{Q}_3}(\alpha_1 - \alpha_2) = v_{\mathbb{Q}_3}(\text{Disc}((x-i)^2+9)) = v_{\mathbb{Q}_3}(-36) = 2,$$

so the lattice type is $[4 : 2]$.

In particular, if J/\mathbb{Q}_3 is the Jacobian of \mathcal{C} and K/\mathbb{Q}_3 a finite extension of residue degree f and ramification degree e , it follows from Theorem 1.2.2 that the Tamagawa number of J/K is given by

$$c_{J/K} = \begin{cases} 2 & \text{if } 2 \nmid f, \\ 4 & \text{if } 2 \parallel f, \\ 4e^2 & \text{if } 4 \mid f. \end{cases}$$

Example 4.1.2. Let \mathcal{C}/\mathbb{Q}_3 be the curve given by

$$y^2 = f(x) = x^6 + 17x^4 + 76x^2 + 36.$$

The polynomial factors as $f(x) = ((x-i)^2+3)((x+i)^2+3)(x^2+9)$ over $\overline{\mathbb{Q}}_3$, so its reduction \bar{f} has 3 double roots, $\alpha = i, \beta = -i, \gamma = 0$. The corresponding tangents are $t_\alpha^\pm = \pm 2, t_\beta^\pm = \pm 2$ and $t_\gamma^\pm = \pm 1$, giving the pairs

$$A^\pm = (i, \pm 2), \quad B^\pm = (-i, \pm 2), \quad C^\pm = (0, \pm 1).$$

The Frobenius orbits on these pairs are $\{A^+, B^+\}, \{A^-, B^-\}, \{C^+\}, \{C^-\}$ and, as in the previous Example, one easily checks that the (scaled) distances in $\overline{\mathbb{Q}}_3$ between the pairs of roots that reduce to α, β and γ are $a=b=1$ and $c=2$. The table now shows the lattice type to be $[1.2_B : 5, 1]$.

If J/\mathbb{Q}_3 is the Jacobian of \mathcal{C} and K/\mathbb{Q}_3 a finite extension of residue degree f and ramification degree e , it follows from Theorem 1.2.2 that the Tamagawa number of J/K is given by

$$c_{J/K} = \begin{cases} 5e & \text{if } 2 \nmid f, \\ 5e^2 & \text{if } 2 \mid f. \end{cases}$$

REFERENCES

- [1] M. Bhargava, B. H. Gross, X. Wang, Pencils of quadrics and the arithmetic of hyperelliptic curves, *J. Amer. Math. Soc.* 30 (2017), 451-493.
- [2] J. Coates, T. Fukaya, K. Kato, R. Sujatha, Root numbers, Selmer groups, and non-commutative Iwasawa theory, *J. Algebr. Geom.* 19, no. 1, 19-97 (2010).
- [3] T. Dokchitser, V. Dokchitser, Regulator constants and the parity conjecture, *Invent. Math.* 178, no. 1 (2009), 23-73.
- [4] T. Dokchitser, V. Dokchitser, Root numbers and parity of ranks of elliptic curves, *J. Reine Angew. Math.* 658 (2011), 39-64.
- [5] T. Dokchitser, V. Dokchitser, Growth of III in towers for isogenous curves, *Compositio Mathematica* 151 (2015), 1981-2005.
- [6] T. Dokchitser, V. Dokchitser, C. Maistret, A. Morgan, Arithmetic of hyperelliptic curves over local fields, preprint (2017).
- [7] A. Grothendieck, Modèles de Néron et monodromie, *LNM* 288, Séminaire de Géométrie 7, Exposé IX, Springer-Verlag, 1973.
- [8] L. H. Halle, J. Nicaise, The Néron component series of an abelian variety, *Math. Ann.* 348, no. 3 (2010) 749-778.

- [9] D. Lorenzini, On the group of components of a Néron model, *J. Reine Angew. Math.* 445 (1993), 109–160.
- [10] A. Morgan, Parity of 2-Selmer ranks of hyperelliptic curves over quadratic extensions, arxiv: 1504.01960.
- [11] Y. Namikawa, K. Ueno, The complete classification of fibres in pencils of curves of genus two, *Manuscripta Math.* 9 (1973), 143–186.
- [12] J. Nekovář, On the parity of ranks of Selmer groups IV, *Compos. Math.* 145 (2009), 1351–1359.
- [13] M. Raynaud, Variétés abéliennes et géométrie rigide, *Actes du congrès international de Nice 1970*, tome 1, 473–477.
- [14] D. Rohrlich, The vanishing of certain Rankin-Selberg convolutions. In: *Automorphic Forms and Analytic Number Theory*, 123–133. Les publications CRM, Montreal (1990).
- [15] D. Rohrlich, Galois theory, elliptic curves, and root numbers. *Compos. Math.* 100 (1996) 311349.
- [16] P. Samuel, *Algebraic Theory of Numbers* (Silberger translation), Kershaw 1971.

KING’S COLLEGE LONDON, STRAND, LONDON, WC2R 2LS, UNITED KINGDOM
E-mail address: `alexander.betts@kcl.ac.uk`

KING’S COLLEGE LONDON, STRAND, LONDON, WC2R 2LS, UNITED KINGDOM
E-mail address: `vladimir.dokchitser@kcl.ac.uk`

KING’S COLLEGE LONDON, STRAND, LONDON, WC2R 2LS, UNITED KINGDOM
E-mail address: `adam.morgan@kcl.ac.uk`